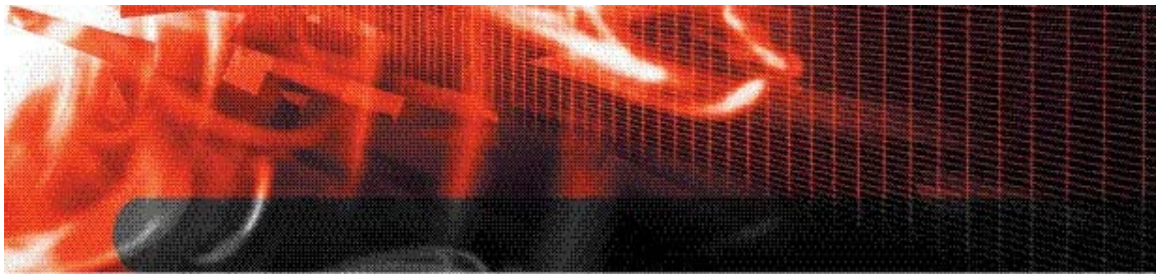


GUIDE D'INSTALLATION

FortiGate-60 / 60M / ADSL, FortiWiFi-60 et FortiGate-100A Version 3.0MR1

FORTINET™

www.fortinet.com

Guide d'installation des FortiGate série 60 et du FortiGate-100A
Version 3.0MR1
10 avril 2006
01-30001-0266-20060410

© Droit d'auteur 2006 Fortinet, Inc. Tous droits réservés. En aucun cas, tout ou partie de cette publication, y compris les textes, exemples, diagrammes ou illustrations, ne peuvent être reproduits, transmis ou traduits, sous aucune forme et d'aucune façon, que ce soit électronique, mécanique, manuelle, optique ou autre, quelqu'en soit l'objectif, sans autorisation préalable de Fortinet, Inc.

Marques déposées
Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyser, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, et FortiWiFi sont des marques déposées de Fortinet, Inc. aux États-Unis et/ou dans d'autres pays. Les noms des sociétés et produits mentionnés ici peuvent être des marques déposées par leurs propriétaires respectifs.

Conformité aux normes
FCC Class A Part 15 CSA/CUS

Attention: Utiliser une batterie du mauvais type pourrait provoquer une explosion. Débarrassez-vous de vos batteries usagées selon la législation locale en vigueur.

Table des Matières

Introduction 7

Gamme de Produits Fortinet 7

Services de souscription FortiGuard 7
FortiClient 8
FortiMail 8
FortiAnalyser 8
FortiReporter 8
FortiBridge 8
FortiManager 9

A propos du FortiGate 9

FortiGate-60/60M/ADSL 9
FortiWiFi-60 9
FortiGate-100A 10

A propos de ce document 10

Conventions utilisées dans ce document 11
Conventions typographiques 11

Documentation FortiGate 11

Base de Connaissance Fortinet (Fortinet Knowledge Center) 13
Remarques sur la documentation technique Fortinet 13

Service clientèle et support technique 13

Installation du FortiGate 14

Inventaire du matériel 14

FortiGate-60/60M/ADSL 14
FortiWiFi-60 15
FortiGate-100A 16
Installation 16

Mise en service du FortiGate 17

Mise hors tension du FortiGate 17

Connexion du FortiGate 18

Interface d'administration web 18
Interface de ligne de commande (CLI) 18
Accès à l'interface d'administration web 18
Tableau de bord du système 20
Interface de ligne de commande (CLI) 21
Connexion à partir de l'interface de ligne de commande 21

Installation rapide à partir de la configuration par défaut 22

Paramétrage par défaut 24

Configuration par défaut du serveur DHCP 24

Configuration réseau par défaut en mode NAT/Route 25

Configuration réseau par défaut en mode Transparent 26

Configuration par défaut du pare-feu 26

Profils de protection par défaut 27

Restauration du paramétrage par défaut ... 28
Restauration du paramétrage par défaut via l'interface d'administration web ... 28
Restauration du paramétrage par défaut à partir de l'interface de ligne de commande ... 28

Configuration du FortiGate pour sa mise en réseau ... 29

Planification de la configuration du FortiGate ... 29
Mode NAT/Route ... 29
Mode NAT/Route avec de multiples connexions externes ... 30
Mode Transparent ... 31

Empêcher l'interface publique du FortiGate de répondre aux requêtes ping ... 32

Installation en mode NAT/Route ... 33
Préparation de la configuration du FortiGate en mode NAT/Route ... 33
Configuration DHCP ou PPPoE ... 34
A partir de l'interface d'administration web ... 35
Configuration des paramètres de base ... 35
Ajout d'une route par défaut ... 36
Vérification de la configuration à partir de l'interface d'administration web ... 36
Tester la connexion ... 36
A partir de l'interface de ligne de commande ... 36
Configuration du FortiGate pour opérer en mode NAT/Route ... 36
Ajout d'une route par défaut ... 38
Tester la connexion ... 38
Connexion du FortiGate au(x) réseau(x) ... 39
Configuration des réseaux ... 40

Installation en mode Transparent ... 41
Préparation de la configuration du FortiGate en mode Transparent ... 41
A partir de l'interface d'administration web ... 41
A partir de l'interface de ligne de commande ... 42
Connexion du FortiGate à votre réseau ... 44
Tester la connexion ... 44

Étapes suivantes ... 45
Paramétrage des date et heure ... 45
Enregistrement de votre FortiGate ... 45
Mise à jour des signatures antivirus et IPS ... 46
Mise à jour des signatures antivirus et IPS à partir de l'interface d'administration web ... 46
Mise à jour des signatures IPS à partir de l'interface de ligne de commande ... 47
Programmation des mises à jour antivirus et IPS ... 47
Ajout d'un serveur override ... 48

Configuration de l'interface modem ... 49

Sélection d'un mode modem ... 49
Configuration en mode redondant ... 49
Configuration en mode stand alone ... 50

Configuration des paramètres du modem ... 51

Connexion et déconnexion du modem en mode stand alone ... 53

Configuration du modem des FortiGate-60 et FortiWiFi-60 ... 53

Ajout d'un serveur Ping ... 56
Détection de l'échec d'une passerelle ... 56

Ajout de règles pare-feu pour les connexions modem ... 56

Configuration de l'interface ADSL 57

Configuration de l'interface ADSL à partir de l'interface d'administration web 57

Configuration des paramètres ADSL de base 57
Configuration DHCP de l'interface ADSL 58
Configuration PPPoE ou PPPoA de l'interface ADSL 59

Configuration de l'interface ADSL à partir de l'interface de ligne de commande 60

Syntaxe de commande 60
Exemple – IPOA ou EOA 63
Exemple – DHCP 64
Exemple – PPPoE ou PPPoA 64

Ajout de règles pare-feu pour les connexions ADSL 64

Utilisation d'un réseau sans fil 65

Installation d'un réseau sans fil 65

Positionnement d'un Point d'Accès 66
Interface Fréquence Radio 66
Utilisation de multiples Points d'Accès 67

Sécurité d'un réseau sans fil 67

Wireless Equivalent Privacy (WEP) 67
Wi-Fi Protected Access (WPA) 68
Mesures de sécurité additionnelles 68
Filtrage des adresses MAC 68
Service Set Identifier 69

Modes d'opération sans fil du FortiWiFi-60 69

Mode Point d'Accès 69
Mode Client 69
Changement de mode d'opération sans fil 70

Installation d'un Point d'Accès FortiWiFi-60 70

Mise en place des paramètres DHCP 70
Mise en place des options de sécurité 71
Configuration des règles pare-feu 72

Logiciel FortiGate 73

Mise à jour logicielle 73

Mise à jour logicielle à partir de l'interface d'administration web 73
Mise à jour logicielle à partir de l'interface de ligne de commande 74

Retour à une version logicielle antérieure 75

Retour à une version logicielle antérieure à partir de l'interface d'administration web 75
Retour à une version logicielle antérieure à partir de l'interface de ligne de commande 76

Mise à jour logicielle à partir d'un redémarrage système et par ligne de commande 78

Restauration de la configuration précédente 80

La clé FortiUSB 81

Mise à jour logicielle à partir de la clé FortiUSB 81
Sauvegarde et restauration à partir de la clé FortiUSB 82
A partir de la fonction d'auto-installation USB 83
Commandes CLI supplémentaires pour l'utilisation de la clé FortiUSB 84

Test d’une nouvelle version logicielle avant son installation 84
Installation et utilisation d’une image logicielle de sauvegarde 86
Installation d’une image logicielle de sauvegarde 86
Index 89

Introduction

Bienvenue et merci d'avoir choisi les produits Fortinet pour la protection en temps réel de votre réseau.

Les boîtiers FortiGate™ Unified Threat Management System (Système de Gestion Unifiée des Attaques) sécurisent les réseaux, réduisent les mauvais usages et abus réseaux, et contribuent à une utilisation plus efficace des ressources de communication, sans compromettre la performance de votre réseau. La gamme a reçu les certifications ICSA pare-feu, VPN IPSec et antivirus.

L'appliance FortiGate est un boîtier entièrement dédié à la sécurité. Il est convivial et fournit une gamme complète de services, que ce soit:

- au niveau des applications (comme le filtrage antivirus et le filtrage de contenu).
- au niveau du réseau (comme le pare-feu, la détection et prévention d'intrusion, les VPN et la qualité de service).

Le système FortiGate utilise la technologie de Dynamic Threat Prevention System (Système Dynamique de Prévention des Attaques) (DTPS™). Celle-ci s'appuie sur les dernières avancées technologiques en matière de conception de microcircuits, de gestion de réseaux, de sécurité et d'analyse de contenu. Cette architecture unique basée sur un Asic permet d'analyser en temps réel les contenus applicatifs et les comportements du réseau.

Gamme de Produits Fortinet

En complément de sa gamme FortiGate, Fortinet propose une solution complète de logiciels et d'appliances de sécurité, adressant notamment la sécurité de la messagerie, la journalisation et l'édition de rapports statistiques, la gestion du réseau et des configurations. Pour plus d'informations sur les gammes de produits Fortinet, vous pouvez consulter le site www.fortinet.com/products.

Services de souscription FortiGuard

Les services FortiGuard sont des services de sécurité développés, mis à jour et gérés par une équipe de professionnels en sécurité Fortinet. Ces services assurent la détection et le filtrage des attaques, même les plus récentes, pour préserver les ordinateurs et les ressources du réseau. Ces services ont été mis au point à partir des plus récentes technologies de sécurité et sont conçus pour opérer à des coûts opérationnels les plus bas possible.

Les services FortiGuard comprennent:

- Le service FortiGuard antivirus
- Le service FortiGuard IPS (Intrusion Prevention System)
- Le service FortiGuard de filtrage web
- Le service FortiGuard antispam
- Le service FortiGuard premier

Sur notre site web, vous trouverez également un scanner de virus et une encyclopédie des virus et attaques.

FortiClient

Le logiciel FortiClient™ offre un environnement informatique sécurisé et fiable aux utilisateurs d'ordinateurs de bureau et d'ordinateurs portables munis des systèmes d'exploitation les plus répandus de Microsoft Windows. FortiClient offre de nombreuses fonctionnalités, y compris:

- un accès VPN pour se connecter aux réseaux distants
- un antivirus temps réel
- une protection contre des modifications du registre Windows
- une recherche des virus sur tout ou partie du disque dur

FortiClient peut s'installer de façon silencieuse et se déployer aisément sur un parc d'ordinateurs selon un paramétrage pré-établi.

FortiMail

FortiMail™ Secure Messaging Platform (Plate-forme de Sécurisation de Messagerie) fournit une analyse heuristique puissante et flexible, de même que des rapports statistiques sur le trafic de mails entrants et sortants. Le FortiMail met en oeuvre des techniques fiables et hautement performantes pour détecter et bloquer les mails non désirés, tels que les signatures SHASH (Spam Hash) ou les filtres bayesians. Construit sur base des technologies primées FortiOS et FortiASIC, FortiMail utilise ses pleines capacités d'inspection de contenu afin de détecter les menaces les plus avancées dans les courriers électroniques.

FortiAnalyser

FortiAnalyser™ fournit aux administrateurs réseaux les informations nécessaires qui leur permettent d'assurer une meilleure protection du réseau, une plus grande sécurité contre attaques et vulnérabilités. FortiAnalyser permet entre autres:

- de centraliser les journaux des boîtiers FortiGate et des serveurs syslog
- de générer des centaines de rapports à partir des données collectées
- de scanner le réseau et générer des rapports de vulnérabilités
- de stocker les fichiers mis en quarantaine par FortiGate

FortiAnalyser peut également être configuré en sniffer réseau et capturer en temps réel le trafic intercepté. Vous pouvez en outre utiliser FortiAnalyser comme lieu de stockage où les utilisateurs peuvent accéder et partager des données, telles que des rapports et journaux conservés sur son disque dur.

FortiReporter

Le logiciel FortiReporter™ Security Analyzer génère des rapports explicites. Il peut centraliser des journaux de n'importe quel boîtier FortiGate, ainsi que de plus de 30 boîtiers de réseau et de sécurité provenant de constructeurs tiers. FortiReporter offre une visibilité sur les abus réseau, l'utilisation de la bande passante et l'usage du web afin de s'assurer que le réseau est utilisé de façon appropriée. FortiReporter permet aux administrateurs d'identifier les attaques et d'y répondre. Il permet également de définir des actions proactives de protection des réseaux avant que ceux-ci ne soient confrontés à une augmentation des menaces.

FortiBridge

FortiBridge™ permet d'assurer une continuité de connexion réseau même en cas de panne électrique d'un système FortiGate. Le FortiBridge connecté en parallèle

au FortiGate dévie le flux réseau lorsqu'il détecte une panne sur le boîtier et reçoit alors le trafic pour éviter toute coupure réseau. FortiBridge est facile à utiliser et à déployer. Vous pouvez programmer à l'avance les actions que FortiBridge mettra en place en cas de panne de courant ou de panne dans le système FortiGate.

FortiManager

FortiManager™ est conçu pour répondre aux besoins des grandes entreprises (y compris les fournisseurs de services de gestion de sécurité) responsables du déploiement et du maintien de dispositifs de sécurité à travers un parc d'équipements FortiGate. FortiManager vous permet de configurer et de contrôler les statuts de plusieurs boîtiers FortiGate. Vous pouvez également consulter leurs journaux en temps réel et leurs historiques, ou encore émettre les versions du microcode FortiOS. FortiManager est facile à utiliser et s'intègre aisément à des systèmes tiers.

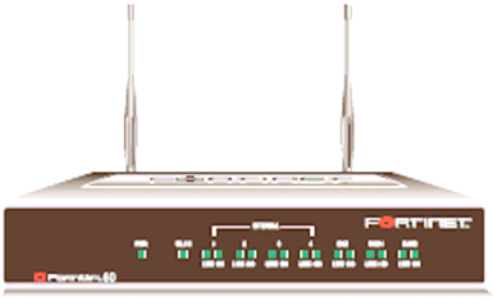
A propos du FortiGate

Les systèmes FortiGate série 60 et le FortiGate-100A, spécifiquement conçus pour les réseaux de petite taille, y compris les bureaux de personnel itinérant, garantissent les mêmes solutions réseaux offertes par tous les boîtiers FortiGate: antivirus, filtrage du contenu web, pare-feu, VPN, et détection et prévention des intrusions sur le réseau. Ces modèles supportent la haute disponibilité.

FortiGate-60/60M/ADSL

Le FortiGate-60 est conçu pour les bureaux de personnel itinérant et les magasins. Il comprend un port modem extérieur qui peut servir de connexion Internet redondante ou stand alone. Le FortiGate-60M comprend quant à lui un modem interne qui peut également servir de connexion Internet redondante ou stand alone. Le FortiGate-60ADSL est pour sa part muni d'un modem ADSL interne.

FortiWiFi-60



Le modèle FortiWiFi est une solution intégrée qui assure des connexions sans fil sécurisées. Il combine mobilité et flexibilité grâce à ses fonctions FortiWiFi Antivirus Firewall. De plus, il s'adapte aux avancées technologiques radiophoniques. Il peut faire office de point de connexion entre réseaux sans fil et réseaux câblés ou tenir lieu de point central d'un réseau sans fil stand alone.

FortiGate-100A

Le FortiGate-100A est une solution pratique et facile à gérer qui répond parfaitement aux applications des petites entreprises, bureaux à domicile et succursales.
Ce boîtier supporte des fonctions avancées telles que VLAN 802.1Q, domaines virtuels et protocoles de routage RIP et OSPF.

A propos de ce document

Ce guide décrit comment installer et configurer un système FortiGate sur votre réseau. Il parcourt également la procédure d'installation et de mise à jour des nouvelles versions logicielles sur votre boîtier FortiGate.

Ce document comprend les chapitres suivants :

- Installation du FortiGate – Décrit l'installation et le démarrage du FortiGate.
- Paramétrage par défaut – Fournit les paramètres par défaut du FortiGate.
- Configuration du FortiGate pour sa mise en réseau – Fournit un aperçu des modes de fonctionnement du FortiGate et explique comment intégrer le FortiGate au réseau.
- Configuration de l'interface modem – Décrit comment configurer et utiliser un modem avec un FortiGate série 60.
- Configuration de l'interface ADSL – Explique comment configurer et utiliser le modem ADSL du FortiGate-60ADSL.
- Utilisation d'un réseau sans fil – Parcourt les considérations concernant les réseaux sans fil et les manipulations qui rendront votre réseau sans fil le plus sécurisé et efficace possible.
- Logiciel FortiGate – Décrit comment installer, mettre à jour, restaurer et tester le microcode du boîtier FortiGate.

Remarque : Ce guide couvre le fonctionnement de cinq boîtiers FortiGate ; Les FortiGate-60/60M, FortiGate-60ADSL , FortiWiFi-60 et FortiGate-100A. Alors que la plupart des informations reprises dans ce guide s'applique à tous les modèles, certaines explications sont spécifiques à un modèle particulier. Une icône telle que ci-dessous fait alors référence au modèle en question.

Conventions utilisées dans ce document

Les conventions suivantes sont utilisées dans ce guide :

- Dans les exemples, les adresses IP privées sont utilisées aussi bien pour les adresses IP privées que publiques.
- Les remarques et attentions fournissent des informations importantes :

Les « **remarques »** vous apportent de l'information additionnelle utile.

Les « **attentions »** vous mettent en garde contre des commandes et procédures qui pourraient avoir des résultats inattendus ou indésirables tels que perte de données ou détérioration de l'équipement.

Conventions typographiques

La documentation du FortiGate utilise les conventions typographiques suivantes :

Convention	Exemple
Entrée clavier	Dans le champ Nom de Passerelle, tapez un nom pour le client VPN distant (par exemple, `Central_Office_1`).

Exemple de code	`config sys global`
	`set ips-open enable`
	`end`

Syntaxe CLI (Interface de ligne de commande)	`config firewall policy`
	`edit id_integer`
	`set http_retry_count <retry_integer>`
	`set natip <address_ipv4mask>`
	`end`

Noms des documents	*Guide d'Administration FortiGate*
Commandes de Menus	Sélectionnez **VPN > IPSEC** et cliquez sur Créer Phase 1.
Affichage du résultat d'un programme	`Welcome!`
Variables	`<address_ipv4>`

Documentation FortiGate

Les versions les plus récentes de la documentation Fortinet, de même que les précédentes parutions, sont disponibles sur le site de documentation technique Fortinet à l'adresse http://docs.forticare.com.

Les guides suivants y sont disponibles en anglais. Certains guides sont ou seront aussi disponibles en français :

- *FortiGate QuickStartGuide - Guide de démarrage rapide FortiGate*
  Fournit les informations de base sur la connexion et l'installation d'un FortiGate
- *FortiGate Install Guide - Guide d'Installation FortiGate*
  Décrit comment installer un FortiGate. Il comprend des informations sur le matériel, des informations sur la configuration par défaut, ainsi que des procédures d'installation, de connexion et de configuration de base. Sélectionnez le guide en fonction du numéro du modèle du produit.
- *FortiGate Administration Guide - Guide d'Administration FortiGate*
  Fournit les informations de base sur la manière de configurer un FortiGate, y compris la définition des profils de protection FortiGate et des règles pare-feu.

Explique comment appliquer les services de prévention d'intrusion, protection antivirus, filtrage web et filtrage antispam (antipollupostage). Parcourt également la manière de configurer un VPN.

- *FortiGate online help - Aide en ligne FortiGate*

  Fournit le *Guide d'Administration* au format HTML avec des outils de recherche. Vous pouvez accéder à l'aide en ligne à partir de l'interface d'administration web.
- *FortiGate CLI Reference - Guide de Référence CLI*

  Décrit comment utiliser l'interface de ligne de commande FortiGate et répertorie toutes ses commandes.
- *FortiGate Log Message Reference - Guide de référence des messages journalisés d'un FortiGate*

  Disponible uniquement à partir de la base de connaissance (Fortinet Knowledge Center), ce mode d'emploi décrit la structure et le contenu des messages présents dans les journaux FortiGate.
- *FortiGate High Availability User Guide - Guide utilisateur des fonctions de haute disponibilité FortiGate*

  Fournit une description détaillée des fonctions de haute disponibilité et du protocole de clustering FortiGate.
- *FortiGate IPS User Guide - Guide utilisateur de l'IPS FortiGate (Système de Prévention d'Intrusion)*

  Décrit la configuration des paramètres IPS FortiGate et le traitement des attaques les plus courantes.
- *FortiGate IPSec VPN User Guide - Guide utilisateur des VPN IPSec FortiGate*

  Fournit des instructions pas à pas sur la configuration VPN IPSec via l'interface d'administration web.
- *FortiGate SSL VPN User Guide - Guide utilisateur du VPN SSL FortiGate*

  Compare les technologies FortiGate VPN IPSec et VPN SSL et décrit comment configurer à partir de l'interface graphique les modes VPN SSL web et VPN SSL tunnel pour les connexions à distance des utilisateurs.
- *FortiGate PPTP VPN User Guide - Guide utilisateur du VPN PPTP FortiGate*

  Explique comment configurer un VPN PPTP via l'interface d'administration web.
- *FortiGate Certificate Management User Guide - Guide utilisateur de gestion des certificats FortiGate*

  Indique comment gérer les certificats digitaux, et notamment comment générer des requêtes de certificat, installer des certificats, importer le certificat de l'autorité de certification et des listes de révocation, sauvegarder et restaurer des certificats et leurs clefs privées associées.
- *FortiGate VLANs and VDOMs User Guide - Guide utilisateur des VLAN et VDOM FortiGate*

  Décrit comment configurer des VLAN et VDOM en mode NAT/Route et Transparent. Des exemples détaillés y sont repris.

Base de Connaissance Fortinet (Fortinet Knowledge Center)

De la documentation technique complémentaire est disponible dans la base de connaissance Fortinet (Fortinet Knowledge Center), notamment des articles sur les dépannages et questions les plus fréquemment rencontrés, des notes techniques, et davantage. Vous pouvez consulter le site de la Base de Connaissance Fortinet à l'adresse http://kc.forticare.com.

Remarques sur la documentation technique Fortinet

Merci d'indiquer toute éventuelle erreur ou omission trouvée dans cette documentation à techdoc@fortinet.com.

Service clientèle et support technique

Le Support Technique Fortinet (Fortinet Technical Support) propose son assistance pour une installation rapide, une configuration facile et une fiabilité des systèmes Fortinet.

Pour connaître ces services, consultez le site de Support Technique Fortinet à l'adresse http://support.fortinet.com.

Installation du FortiGate

Cette section couvre l'installation et le déploiement du FortiGate sur votre réseau. Les sujets suivants sont parcourus dans cette section:

- Inventaire du matériel
- Installation
- Mise en service du FortiGate
- Connexion du FortiGate

Inventaire du matériel

Cette section répertorie les composants matériels du système FortiGate afin de s'assurer que le matériel livré est complet.

FortiGate-60/60M/ADSL

Le contenu de la boîte du FortiGate-60/60M/ADSL se compose des articles suivants :

- Le boîtier FortiGate-60 Unified Threat Management System
- Un câble Ethernet croisé orange (numéro de l'article Fortinet CC300248)
- Un câble Ethernet classique gris (numéro de l'article Fortinet CC300249)
- Un câble série RJ-45 <> DB-9 (numéro de l'article Fortinet CC300247)
- Un câble téléphonique RJ-11 (uniquement pour le FortiGate-60M)
- Un câble d'alimentation et un adaptateur secteur
- Le Guide de démarrage rapide FortiGate-60, le Guide de démarrage rapide FortiGate-60M ou le Guide de démarrage rapide FortiGate-60ADSL
- Un CD de documentation Fortinet

Illustration 1 : Articles du FortiGate-60/60M

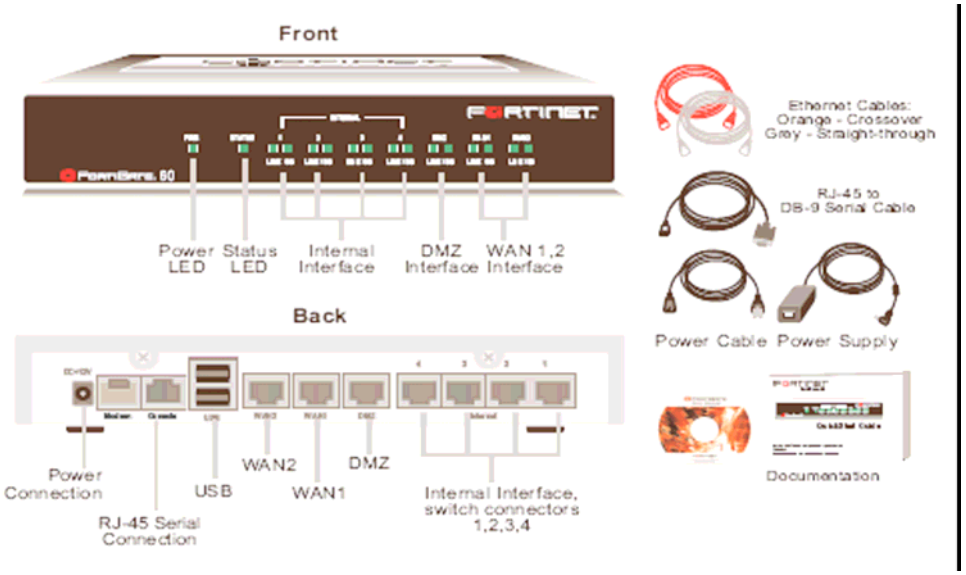


Tableau 1 : Spécifications techniques

Dimensions	21.9 x 15.6 x 3.5 cm (8.63 x 6.13 x 1.38 pouces)
Poids	0.68 kg (1.5 livres)
Conditions de puissance	Tension d'entrée : 12 Volts Courant d'entrée : 3 A
Spécifications sur l'environnement	Température de fonctionnement : 0 à 40°C (32 à 104°F) Température de stockage : -25 à 70°C (-13 à 158°F) Humidité : 5 à 95% non condensée

FortiWiFi-60

Le contenu de la boîte du FortiWiFi-60 se compose des articles suivants :

- Le boîtier FortiWiFi-60 Unified Threat Management System
- Un câble Ethernet croisé orange (numéro de l'article Fortinet CC300248)
- Un câble Ethernet classique gris (numéro de l'article Fortinet CC300249)
- Un câble série RJ-45 <> DB-9 (numéro de l'article Fortinet CC300247)
- Un câble d'alimentation et un adaptateur secteur
- Le Guide de démarrage rapide FortiWiFi-60
- Un CD de documentation Fortinet

Illustration 2 : Articles du FortiWiFi-60/60M

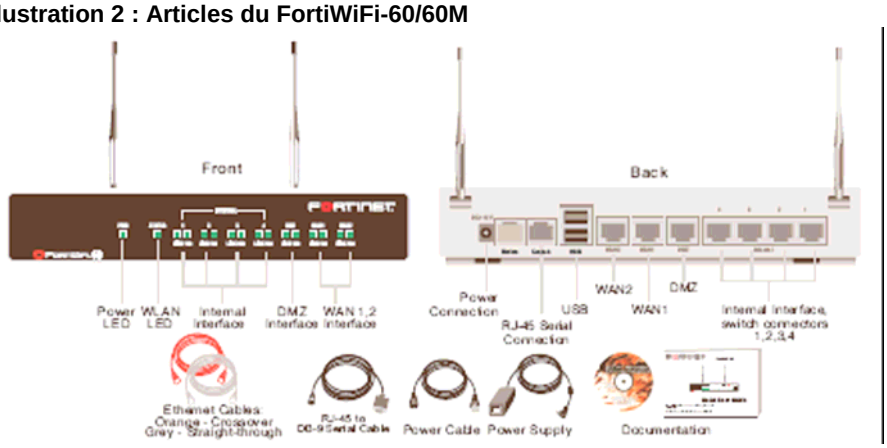


Tableau 2 : Spécifications techniques

Dimensions	21.9 x 15.6 x 3.5 cm (8.63 x 6.13 x 1.38 pouces)
Poids	0.68 kg (1.5 livres)
Conditions de puissance	Tension d'entrée : 12 Volts Courant d'entrée : 3 A
Connectivité sans fil	Type d'antenne : double antenne fixe externe Gamme de fréquence de l'antenne: 802.11 b/g :2.4GHz Gain d'antenne : 5dBi
Spécifications sur l'environnement	Température de fonctionnement : 0 à 40°C (32 à 104°F) Température de stockage : -25 à 70°C (-13 à 158°F) Humidité : 5 à 95% non condensée

FortiGate-100A

Le contenu de la boîte du FortiGate-100A se compose des articles suivants :

- Le boîtier FortiGate-100A Unified Threat Management System
- Un câble Ethernet croisé orange (numéro de l'article Fortinet CC300248)
- Un câble Ethernet classique gris (numéro de l'article Fortinet CC300249)
- Un câble série RJ-45 <> DB-9 (numéro de l'article Fortinet CC300302)
- Un câble d'alimentation et un adaptateur secteur
- Le Guide de démarrage rapide FortiGate-100A
- Un CD de documentation Fortinet

Illustration 3 : Articles du FortiGate-100A

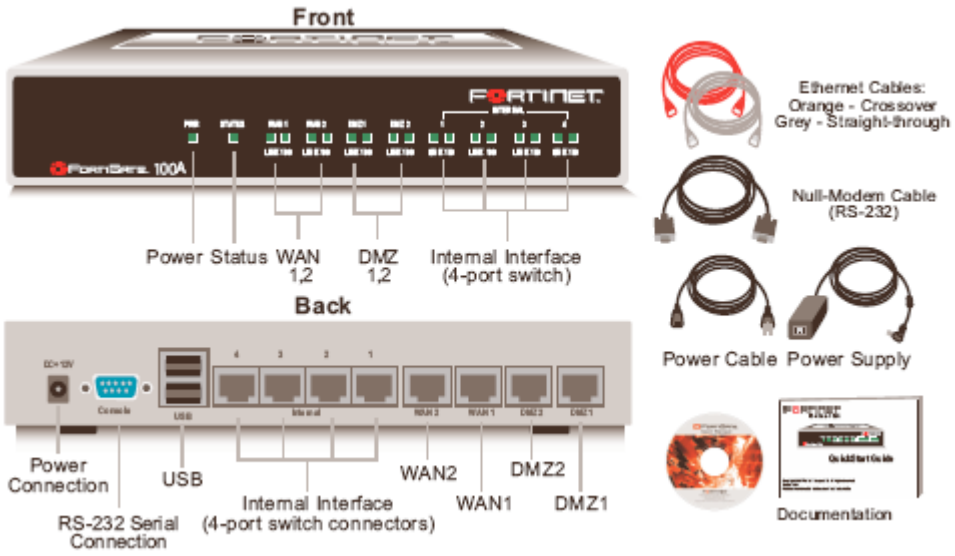


Tableau 3 : Spécifications techniques

Dimensions	26 x 15.6 x 3.5 cm (10.25 x 6.13 x 1.75 pouces)
Poids	0.8 kg (1.75 livres)
Conditions de puissance	Tension d'entrée : 12 Volts Courant d'entrée : 5 A
Spécifications sur l'environnement	Température de fonctionnement : 0 à 40°C (32 à 104°F) Température de stockage : -25 à 70°C (-13 à 158°F) Humidité : 5 à 95% non condensée

Installation

Le boîtier FortiGate doit être installé sur une surface plate et stable. Assurez-vous que les côtés du boîtier FortiGate ont au moins 3.75 cm (1.5 pouce) d'espace afin de permettre une circulation d'air et un refroidissement adéquats.

Mise en service du FortiGate

Les boîtiers FortiGate ne sont pas équipés d'un interrupteur marche/arrêt (on/off).

Mettre en service un boîtier FortiGate

1. Connectez l'adaptateur secteur à la fiche d'alimentation au dos du boîtier FortiGate.
2. Connectez l'adaptateur secteur au câble d'alimentation.
3. Connectez le câble d'alimentation à une prise de courant.

Le boîtier FortiGate se met en route et les diodes électroluminescentes « POWER » (ALIMENTATION) et « STATUS » (STATUT) s'allument. La diode de STATUS clignote pendant la mise en marche du boîtier FortiGate et reste allumée pendant tout le fonctionnement du système.

Tableau 4 : Les indicateurs des diodes électroluminescentes

Diode	État	Description
Power	Vert	Le boîtier FortiGate est sous tension.
	Éteint	Le boîtier FortiGate est hors tension.
Status	Clignotant	Le boîtier FortiGate est en phase de démarrage.
	Vert	Le boîtier FortiGate fonctionne normalement.
	Éteint	Le boîtier FortiGate est hors tension.
Link (internal DMZ1 DMZ2 WAN 1 WAN 2)	Vert	Le câble approprié est utilisé et l'équipement connecté alimenté.
	Vert – clignotant	Activité réseau présente sur cette interface.
	Éteint	Pas de lien établi.
DMZ1 DMZ2 WAN 1 WAN 2	Vert	L'interface est connectée à 100 Mbit/s.

Mise hors tension du FortiGate

Assurez-vous que le système d'exploitation FortiGate a été éteint correctement avant de mettre le boîtier hors tension, ceci afin d'éviter des problèmes éventuels.

Mettre le boîtier FortiGate hors tension

1. - À partir de l'interface d'administration web, allez dans **Système > Statut > System Operation**, sélectionnez Eteindre (Shut down), cliquez ensuite sur Go.
   - À partir des commandes CLI :
   ```
   execute shutdown
   ```
2. Déconnectez le câble d'alimentation de la source d'alimentation.

Connexion du FortiGate

Deux méthodes permettent la connexion et configuration des paramètres de base du FortiGate :

- L'interface d'administration web
- L'interface de ligne de commande (CLI)

Interface d'administration web

Vous pouvez configurer et gérer le FortiGate avec une connexion HTTP ou HTTPS, à partir de tout ordinateur muni de Microsoft Internet Explorer 6.0 ou de tout autre navigateur récent. L'interface d'administration web fonctionne en plusieurs langues.

L'interface d'administration web permet la configuration et la gestion de la plupart des paramètres FortiGate.

Interface de ligne de commande (CLI)

Vous pouvez accéder à l'interface de ligne de commande FortiGate en connectant le port série de votre ordinateur au port console du FortiGate. Vous pouvez également avoir recours à Telnet ou à une connexion sécurisée SSH pour vous connecter en CLI à partir de n'importe quel réseau connecté au FortiGate, y compris Internet.

Accès à l'interface d'administration web

La procédure suivante retrace les étapes pour une première connexion à l'interface d'administration web. Les changements de configuration apportés via l'interface d'administration web sont instantanément pris en compte, sans qu'il soit nécessaire de réinitialiser le pare-feu et sans interruption de service.

Pour vous connecter à l'interface d'administration web, vous devez disposer :

- d'un ordinateur avec une connexion Ethernet
- de Microsoft Internet Explorer version 6.0 ou plus ; ou toute récente version de navigateur web
- d'un câble Ethernet croisé ou d'un concentrateur Ethernet et deux câbles Ethernet

Remarque : Avant de démarrer Internet Explorer (ou toute autre version d'un navigateur répandu), vérifier sur votre boîtier FortiGate que la connexion physique entre l'ordinateur et le boîtier FortiGate fonctionne correctement.

Se connecter à l'interface d'administration web

1 Configurez votre ordinateur avec l'adresse IP statique 192.168.1.2 et le masque de réseau 255.255.255.0.

Vous pouvez configurer votre ordinateur d'administration afin d'obtenir automatiquement une adresse IP via DHCP. Le serveur FortiGate DHCP affecte une adresse IP à l'ordinateur d'administration dans l'intervalle 192.168.1.1 à 192.168.1.254.

2 A l’aide des câbles croisés ou d’un concentrateur et câbles Ethernet, connectez l’interface interne de votre FortiGate à la connexion Ethernet de l’ordinateur.

3 Démarrez Internet Explorer et entrez l’adresse https://192.168.1.99 (n’oubliez pas d’inclure le « s » dans https://).

Pour assurer une méthode sécurisée d’authentification HTTPS, le FortiGate dispose d'un certificat de sécurité auto-signé, et il lui est envoyé aux clients distants à chaque fois qu’ils initient une connexion HTTPS vers le FortiGate. Lors de l’établissement de la connexion, le FortiGate affiche deux alertes dans la fenêtre du navigateur.

La première alerte vous demande d’accepter et d’installer, à titre facultatif, le certificat de sécurité auto-signé FortiGate. Si vous refusez ce certificat, le FortiGate refuse la connexion. Si vous l’acceptez, la page d’ouverture de la session du FortiGate s’affiche. Les informations de connexion (compte administrateur et mot de passe) sont chiffrées avant d’être envoyées au FortiGate. Si vous choisissez d’accepter le certificat de manière permanente, l’alerte n’apparaîtra plus.

Juste avant l’affichage de la page d’ouverture de la session, une deuxième alerte vous informe que le nom du certificat FortiGate diffère de celui de la demande originale. Cette alerte se produit car le FortiGate redirige la connexion. C’est un message informatif. Sélectionnez OK pour continuer l’ouverture de la session.

Illustration 4 : Ouverture d'une session sur le FortiGate

4 Tapez `admin` dans le champ Nom et cliquez sur Login.

Tableau de bord du système

Une fois la connexion à l'interface d'administration web établie, la fenêtre de navigation affiche le tableau de bord du système qui reprend tous les statuts du système.

Illustration 4 : Tableau de bord du système FortiGate-60M

Le tableau de bord reprend les informations suivantes :

- Statut des Ports (Port Status) – le tableau de bord affiche la face avant du boîtier FortiGate, ainsi que le statut de la connexion au FortiAnalyser - un X indiquant une absence de connexion, un V la présence de connexion. Le FortiLog apparaît en gris en cas d'absence de connexion du FortiGate au FortiLog. En plaçant le curseur de la souris sur un des ports, les informations suivantes sur son statut s'affichent:
  - le statut du port (up ou down)
  - l'adresse IP et le masque de réseau
  - la vitesse et le nombre total de paquets envoyés et reçus

  Chaque port actif apparaît en vert.
- Information système (System Information) – regroupe les informations sur le système d'exploitation telles que le numéro de série du boîtier et la version de code. Cette zone vous permet de mettre à jour le logiciel, de programmer la date et l'heure et de changer de mode de fonctionnement.
- Ressources du système (System Resources) – permet de surveiller l'utilisation des ressources du boîtier.
- Statut des licences (License Information) – affiche les mises à jour actuelles des antivirus et des systèmes de sécurité de votre FortiGate.
- Console de Messages d'Alerte (Alert Message Console) - affiche les messages d'alerte des événements récents.
- Statistiques (Statistics) – fournit les informations statistiques en temps réel sur le trafic et les attaques.

Interface de ligne de commande (CLI)

Vous pouvez accéder à l'interface de ligne de commande FortiGate en connectant le port série de votre ordinateur au port console du FortiGate. Vous pouvez également avoir recours à Telnet ou à une connexion sécurisée SSH pour vous connecter en CLI à partir de n'importe quel réseau connecté au FortiGate, y compris Internet.

L'interface de ligne de commande offre les mêmes fonctionnalités de configuration et de surveillance que l'interface d'administration web. Cependant, les commandes CLI servent également à la configuration d'options avancées, non disponibles à partir de l'interface graphique. Ce guide décrit certaines commandes CLI de base et avancées. Pour une description plus complète des modalités de connexion et des commandes de l'interface de ligne de commande, consulter le *Guide de Référence CLI*.

Connexion à partir de l'interface de ligne de commande

Comme alternative à l'interface graphique, vous pouvez installer et configurer le FortiGate à partir de l'interface de ligne de commande. Les changements apportés dans la configuration à partir de l'interface de ligne de commande sont instantanément pris en compte, sans qu'il soit nécessaire de réinitialiser le pare-feu et sans interruption de service.

Pour vous connecter en CLI au FortiGate, vous devez disposer:

- d'un ordinateur avec un port de communication disponible
- du câble série RJ-45 <> DB-9 inclus avec le matériel livré
- d'un logiciel d'émulation terminal tel que l'HyperTerminal de Microsoft Windows

Remarque : La procédure suivante s'appuie sur le logiciel Microsoft Windows HyperTerminal. Vous pouvez appliquer la même procédure avec tout programme d'émulation terminal.

Se connecter en CLI :

1. Connectez votre câble série RJ-45 <> DB-9 au port de communication (port série) de votre ordinateur d'une part et au port de la console du FortiGate d'autre part.
2. Démarrez le logiciel HyperTerminal, entrez un nom pour la connexion et cliquez sur OK.
3. Configurez l'HyperTerminal afin de vous connecter directement au port de communication de votre ordinateur et cliquez sur OK.
4. Sélectionnez les paramètres suivants du port et cliquez ensuite sur OK :

Bits par seconde	9600
Bits de données	8
Parité	Aucune
Bits d'arrêt	1
Contrôle de flux	Aucun

5. Appuyez sur la touche Enter pour vous connecter en CLI au FortiGate. Le message d'ouverture de la session apparaît.
6. Tapez `admin` et appuyez deux fois sur la touche Enter.

   Le message suivant s'affiche :

   ```
   Welcome !
   ```

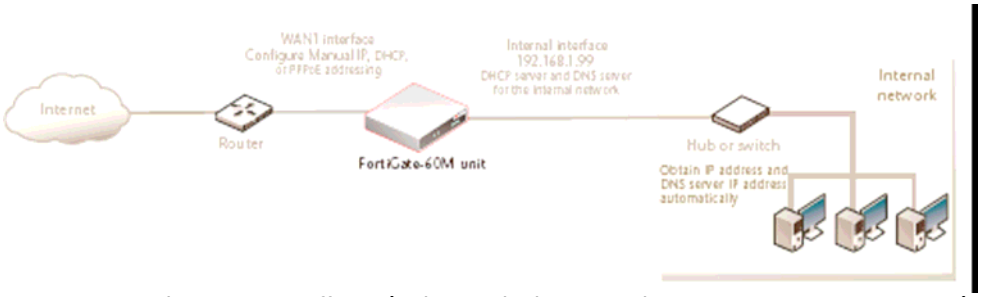
   Tapez ? pour afficher les commandes disponibles. Pour plus d'informations à propos de l'utilisation de l'interface de ligne de commande, reportez-vous au *Guide de Référence CLI.*

Installation rapide à partir de la configuration par défaut

Vous pouvez rapidement installer votre boîtier FortiGate, pour une utilisation privée ou professionnelle, à l'aide de l'interface d'administration web et à partir de la configuration par défaut. Pour ce faire, configurez vos ordinateurs de manière à leurs affecter une adresse IP, ainsi que des adresses IP du serveur DNS automatiquement (via DHCP). Ensuite, accédez à l'interface d'administration web et configurez les paramètres nécessaires de l'interface WAN1. Vous pouvez également configurer des serveurs DNS FortiGate et ajouter une route par défaut si nécessaire.

L'interface interne du FortiGate agit comme un serveur DHCP pour le réseau interne, affectant automatiquement des adresses IP aux ordinateurs (jusqu'à 100 ordinateurs) dans l'intervalle entre 192.168.1.110 – 192.168.1.210.

Illustration 6 : Configuration rapide à partir des paramètres par défaut



Le serveur FortiGate DHCP affecte également l'adresse IP du serveur DNS 192.168.1.99 à chaque ordinateur du réseau interne. De cette manière, l'interface interne du boîtier FortiGate agit comme un serveur DNS pour le réseau interne.
Au moyen d'un relayage DNS, le FortiGate transfère les requêtes DNS reçues par le réseau interne vers les adresses IP du serveur DNS ajoutées à la configuration du FortiGate et renvoie les résultats vers le réseau interne.

Pour plus d'informations sur les paramètres par défaut du serveur DHCP, voir « Configuration par défaut du serveur DHCP » à la page 24.

La procédure suivante décrit comment configurer votre réseau interne et le FortiGate afin de pouvoir utiliser la configuration par défaut.

1. Connectez votre boîtier FortiGate entre votre réseau interne et Internet. Mettez-le ensuite sous tension.
2. Etablissez les propriétés TCP/IP sur les ordinateurs du réseau pour une affectation automatique d'une adresse IP et d'une adresse IP pour le serveur DNS (via DHCP).
3. A partir de l'ordinateur d'administration, connectez-vous à l'adresse : https://192.168.1.99. L'interface d'administration web apparaît.
4. Sélectionnez **Système > Réseau > Interface** et cliquez sur le bouton Editer de l'interface externe.
5. Sélectionnez un des modes d'adressage suivants :
   - Manuel : Entrez une adresse IP et un masque de réseau statiques, sélectionnez OK et passez au point 6.
   - DHCP : Pour obtenir une adresse IP de votre fournisseur d'accès Internet (FAI), sélectionnez DHCP et passez au point 9.
   - PPPoE : Pour obtenir une adresse IP de votre fournisseur d'accès Internet, sélectionnez PPPoE et passez au point 9.
6. Sélectionnez **Système > Réseau > DNS**.
7. Choisissez un des paramètres DNS suivants :
   - Obtenir dynamiquement les adresses des serveurs DNS: pour obtenir les adresses DNS via votre FAI, cochez cette case et cliquez sur Appliquer.

- Utiliser les adresses des serveurs DNS suivants: entrez les adresses fournies par votre FAI et cliquez sur Appliquer.

8 Sélectionnez **Routage > Route statique**, cliquez sur le bouton Editer de la route # 1, changez la Passerelle par l'adresse IP de la passerelle par défaut de votre FAI et cliquez sur OK.

La configuration du réseau est terminée. Vous pouvez passer maintenant au chapitre « Etapes suivantes » à la page 45.

9 Cochez les options « Obtenir dynamiquement la route par défaut » et « Remplacer le serveur DNS préconfiguré » si votre FAI les supportent. Cliquez sur OK et passez maintenant au chapitre "Etapes suivantes" à la page 45.

Allez au point 6 si vous n'utilisez pas ces options.

Paramétrage par défaut

Le FortiGate vous est fourni avec une configuration par défaut qui vous permet de vous connecter à l'interface d'administration web et de configurer l'accès du boîtier au réseau. Pour cela, vous devez entrer un mot de passe administrateur, modifier les adresses IP de l'interface du réseau, compléter les adresses IP du serveur DNS, et, si nécessaire, configurer le routage de base.

Si vous pensez utiliser votre FortiGate en mode Transparent, commencer d'abord par changer le mode de fonctionnement pour ensuite configurer l'accès du FortiGate au réseau.

Une fois le paramétrage réseau terminé, vous pourrez configurer d'autres paramètres, comme les date et heure, la mise à jour des bases de connaissance antivirus et IPS, et procéder à l'enregistrement du boîtier.

La configuration par défaut de votre pare-feu comprend une seule règle NAT (Network Address Translation) qui permet aux utilisateurs du réseau interne de se connecter au réseau externe et empêche les utilisateurs du réseau externe de se connecter au réseau interne. Vous pouvez étendre vos règles pare-feu en vue de contrôler davantage le trafic du réseau passant par le FortiGate.

Les profils de protection par défaut servent à la mise en place de différents niveaux de sécurité (antivirus, filtrage de contenu, filtrage antispam, et prévention d'intrusion) du trafic contrôlé par les règles pare-feu.

Ce chapitre couvre les sujets suivants :

- Configuration par défaut du serveur DHCP
- Configuration réseau par défaut en mode NAT/Route
- Configuration réseau par défaut en mode Transparent
- Configuration par défaut du pare-feu
- Profils de protection par défaut
- Restauration du paramétrage par défaut

Configuration par défaut du serveur DHCP

Les paramètres par défaut du serveur DHCP permettent une configuration rapide du réseau interne et du boîtier FortiGate. Voir « Installation rapide à partir de la configuration par défaut » à la page 22.

Tableau 5 : Configuration par défaut du serveur DHCP FortiGate

Nom	internal_dhcp_server
Interface	Internal
Passerelle par défaut	192.168.1.99
Plage d'adresses IP	192.168.1.110 – 192.168.1.210
Masque de réseau	255.255.255.0
Durée du Bail	7 jours
Serveur DNS 1	192.168.1.99

Configuration réseau par défaut en mode NAT/Route

Lorsque le FortiGate est mis sous tension pour la première fois, il fonctionne en mode routé (NAT/Route) avec une configuration réseau par défaut telle que détaillée dans le tableau 6 ci-dessous. Cette configuration vous permet d'utiliser l'interface graphique du FortiGate et d'établir la configuration requise pour connecter le FortiGate au réseau. Dans ce même tableau les droits d'administration HTTPS signifient que vous pouvez vous connecter à l'interface graphique en utilisant le protocole HTTPS. Lorsque la commande ping est spécifiée dans les droits d'accès, cela signifie que cette interface répond aux requêtes ping.

Tableau 6 : Configuration réseau par défaut en mode NAT/Route

Compte administrateur	Nom de l'utilisateur : Mot de passe :	admin (néant)
Interface Interne	IP : Masque de réseau : Droits d'administration :	192.168.1.99 255.255.255.0 HTTP, HTTPS, Ping
Interface WAN1	IP : Masque de réseau : Droits d'administration :	192.168.100.99 255.255.255.0 Ping
Interface WAN2	IP : Masque de réseau : Droits d'administration :	192.168.101.99 255.255.255.0 Ping
Interface DMZ **DMZ1** **(FortiGate-100A)**	IP : Masque de réseau : Droits d'administration :	10.10.10.1 255.255.255.0 HTTPS, Ping
Interface DMZ2 **(FortiGate-100A)**	IP : Masque de réseau : Droits d'administration :	0.0.0.0. 0.0.0.0. Ping
Interface modem	IP : Masque de réseau : Droits d'administration :	0.0.0.0. 0.0.0.0.
Interface Modem ADSL	IP : Masque de réseau : Droits d'administration :	0.0.0.0. 0.0.0.0.
WLAN	IP : Masque de réseau : Droits d'administration :	10.10.80.1 255.255.255.0 Ping
Paramètres du réseau	Passerelle par défaut (pour route par défaut)	192.168.100.1
	Interface connectée au réseau externe (pour route par défaut)	Externe
	Route par défaut Une route par défaut est constituée d'une passerelle par défaut et de l'interface connectée au réseau extérieur (Internet généralement). Ces paramètres dirigent tout le trafic non local vers cette interface et le réseau externe.	
	DNS primaire	65.39.139.53
	DNS secondaire	65.39.139.63

Configuration réseau par défaut en mode Transparent

En mode Transparent, le FortiGate fonctionne avec une configuration réseau telle que détaillée dans le tableau 7 ci-dessous.

Tableau 7 : Configuration réseau par défaut en mode Transparent

Compte administrateur	Nom d'utilisateur : Mot de passe :	admin (néant)
IP d'administration	IP : Masque de réseau :	0.0.0.0. 0.0.0.0.
DNS	Serveur DNS primaire : Serveur DNS secondaire :	65.39.139.53 65.39.139.63
Droits d'administration	Interne DMZ DMZ1 DMZ2 WAN1 WAN2 WLAN	HTTPS, Ping HTTPS, Ping HTTPS, Ping Ping Ping Ping Ping

Configuration par défaut du pare-feu

Les règles pare-feu du FortiGate déterminent les critères d'accès ou de rejet des flux réseau par le FortiGate. La configuration par défaut contient une seule règle pare-feu qui permet à tout le trafic provenant du réseau interne d'accéder à Internet. Tant qu'aucune autre règle n'est définie, aucun autre trafic n'est accepté par le FortiGate. Pour permettre au trafic de traverser le boîtier FortiGate, vous pouvez ajouter des règles pare-feu. Reportez-vous au *Guide d'Administration FortiGate* pour plus d'informations sur l'ajout de règles pare-feu.

Les paramètres suivants sont préconfigurés dans la configuration par défaut afin de faciliter l'ajout de règles pare-feu.

Tableau 8 : Configuration par défaut du pare-feu

Paramètres de configuration	**Nom**	**Description**
Règle pare-feu	Interne -> Externe	Source : Toutes Destination : Toutes
Adresse	All	Représente toute valeur d'adresse réseau.
Service	Plus de 50 services prédéfinis	Sélectionnez les services désirés parmi les 50 services prédéfinis pour contrôler le trafic reçu.
Plage horaire	Toujours (Always)	Une plage récurrente est valable à tout moment.
Profil de Protection	Strict, scan, web, unfiltered	Définit quels sont les services de sécurité additionnels qui doivent être appliqués au flux: antivirus, filtrage web antispam, et IPS.

La configuration par défaut du pare-feu est la même dans les modes NAT/Route et Transparent.

Profils de protection par défaut

Vous pouvez définir plusieurs profils de protection auxquels vous appliquez des niveaux de protection différenciés du trafic contrôlé par le FortiGate. Vous pouvez utiliser des profils de protection pour :

- appliquer un contrôle antivirus aux règles HTTP, FTP, IMAP, POP3 et SMTP
- activer du filtrage Web statique sur les règles HTTP
- appliquer du filtrage web dynamique, par catégorie, sur ces mêmes règles HTTP
- activer les services antispam sur les règles IMAP, POP3 et SMTP
- activer les services de prévention d'intrusion sur tous les flux
- activer la journalisation de contenu pour les flux HTTP, FTP, IMAP, POP3 et SMTP

Les profils de protection permettent la création de différents types de protection qui vont s'appliquer à différentes règles pare-feu.
Par exemple, alors que le trafic entre des zones interne et externe nécessite une protection stricte, le trafic entre zones de confiance internes peut n'avoir besoin que d'une protection modérée. Vous pouvez configurer des règles pare-feu dans le but d'utiliser des profils de protection identiques ou différents selon les flux.

Des profils de protection sont disponibles en mode routé et transparent.

Quatre profils de protection sont préconfigurés:

Strict	Applique une protection maximum pour le trafic HTTP, FTP, IMAP, POP3 et SMTP. Vous n'utiliserez probablement pas ce profil rigoureux de protection en circonstances normales mais il est disponible en cas de problème de virus nécessitant une analyse maximum.
Scan	Applique une analyse antivirus et une mise en quarantaine de fichiers du contenu du trafic HTTP, FTP, IMAP, POP3 et SMTP.
Web	Applique une analyse antivirus et un blocage du contenu web. Vous pouvez ajouter ce profil de protection aux règles pare-feu qui contrôlent le trafic HTTP.
Unfiltered (Non filtré)	N'applique ni analyse, ni blocage, ni IPS. A utiliser dans le cas où aucune protection du contenu du trafic n'est souhaitée. Vous pouvez ajouter ce profil de protection aux règles pare-feu pour les connexions entre des réseaux hautement fiables et sécurisés dont le contenu ne nécessite pas d'être protégé.

Restauration du paramétrage par défaut

Si vous avez fait une erreur de configuration et que vous n'arrivez pas à la corriger, vous pouvez toujours restaurer les paramètres par défaut et recommencer la configuration.

Attention : Cette procédure supprime tous les changements apportés à la configuration du FortiGate et rétablit les paramètres par défaut, y compris ceux des interfaces, comme les adresses IP.

Restauration du paramétrage par défaut via l'interface d'administration web

Rétablir les paramètres par défaut

1. Allez dans **Système > Statut > System Operation**.
2. Sélectionnez Réinitialiser aux paramètres par défaut.
3. Cliquez sur Go.

Restauration du paramétrage par défaut à partir de l'interface de ligne de commande

Pour rétablir les paramètres par défaut, utilisez la commande suivante :

```
execute factoryreset
```

Configuration du FortiGate pour sa mise en réseau

Cette section vous donne un aperçu des modes de fonctionnement du FortiGate. Avant de procéder à la configuration du FortiGate, il est important de planifier la manière dont vous allez l'intégrer sur le réseau. La planification de la configuration dépend du mode de fonctionnement sélectionné : le mode NAT/Route ou le mode Transparent.

Cette section traite les sujets suivants:

- Planification de la configuration du FortiGate
- Empêcher l'interface publique du FortiGate de répondre aux requêtes ping
- Installation en mode NAT/Route
- Installation en mode Transparent
- Étapes suivantes

Planification de la configuration du FortiGate

Avant de procéder à la configuration du FortiGate, il est nécessaire de planifier l'intégration du boîtier au réseau, et de décider, notamment :

- de la visibilité de votre équipement sur le réseau
- des fonctions pare-feu à fournir
- du contrôle à appliquer au trafic

La planification de la configuration dépend du mode de fonctionnement sélectionné: le mode NAT/Route (par défaut) ou le mode Transparent.

Vous pouvez également configurer le FortiGate et le réseau qu'il protège en gardant le paramétrage par défaut.

Mode NAT/Route

En mode routé, le FortiGate est visible sur le réseau. De même que pour un routeur, ses interfaces sont présentes sur différents sous-réseaux. Dans ce mode, les interfaces suivantes sont disponibles :

- WAN1 : interface réseau externe (généralement Internet)
- Internal : interface réseau interne
- Modem est l'interface pour la connexion d'un modem externe pour les FortiGate série 60
- ADSL est l'interface du modem ADSL interne du FortiGate-60ADSL
- DMZ est l'interface vers une DMZ
- WLAN est l'interface vers les LAN sans fil des boîtiers FortiWiFi

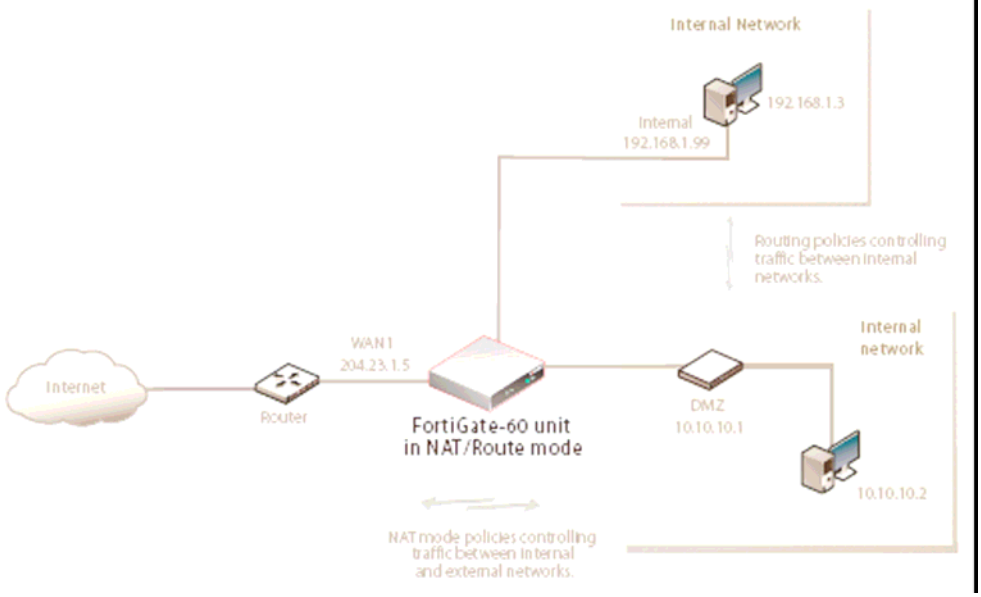
Vous pouvez ajouter des règles pare-feu pour vérifier si le FortiGate opère en mode NAT ou en mode Transparent. Ces règles contrôlent la circulation du trafic en se basant sur les adresses sources et de destination, ainsi que sur les protocoles et ports applicatifs de chaque paquet. En mode NAT, le FortiGate exécute une translation des adresses du réseau avant d'envoyer le paquet vers le réseau de destination. En mode Transparent, il n'y a pas de translation d'adresses.

Le mode NAT/Route est généralement utilisé lorsque le FortiGate opère en tant que passerelle entre réseaux privés et publics. Dans cette configuration, vous pouvez activer de la translation d'adresse au niveau des règles pare-feu qui

contrôlent le trafic circulant entre les réseaux interne et externe (généralement Internet).

Remarque : Vous pouvez créer des règles pare-feu en mode route pour gérer le trafic circulant entre plusieurs réseaux internes, par exemple entre une zone démilitarisée et votre réseau interne.

Illustration 7 : Exemple de configuration réseau d'un FortiGate-60 en mode NAT/Route



Mode NAT/Route avec de multiples connexions externes

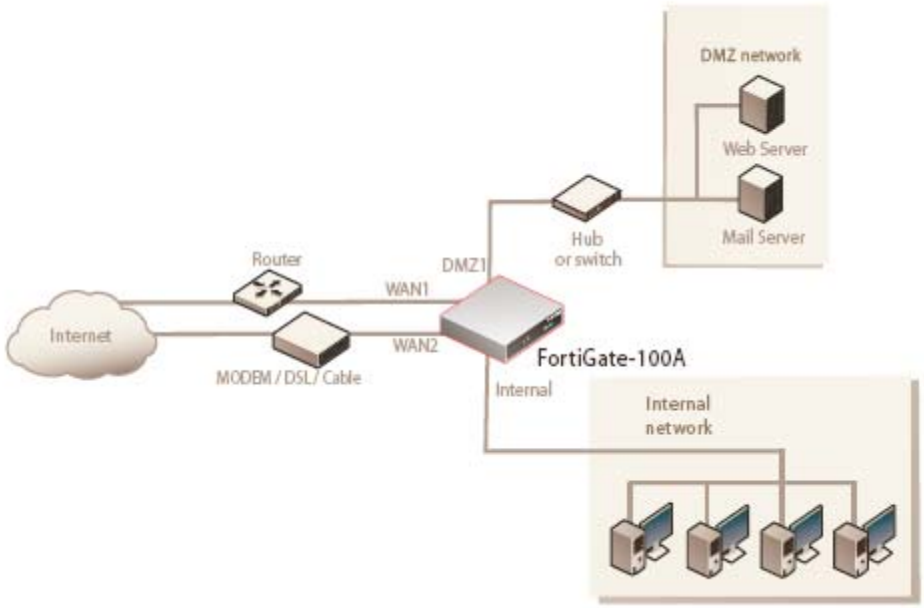
En mode routé, le FortiGate peut se configurer avec des connexions multiples et redondantes au réseau externe.
Vous pourriez, par exemple, créer la configuration suivante :

- WAN1 pour l'interface par défaut du réseau externe (généralement Internet)
- Modem pour l'interface redondante du réseau externe pour les FortiGate série 60
- DMZ pour l'interface redondante du réseau externe pour le FortiGate-100A
- Internal pour l'interface du réseau interne

Votre configuration doit permettre au routage de supporter des connexions Internet redondantes. Le routage peut automatiquement rediriger les connexions d'une interface dans le cas où la connexion au réseau externe échoue.

Par ailleurs, la configuration de règles de sécurité est la même que pour une configuration en mode routé avec une seule connexion Internet. Vous établirez des règles pare-feu en mode NAT pour contrôler le trafic circulant entre les réseaux interne et externe.

Illustration 8 : Exemple de configuration de multiples connexions Internet en mode NAT/Route pour un FortiGate-100A



Mode Transparent

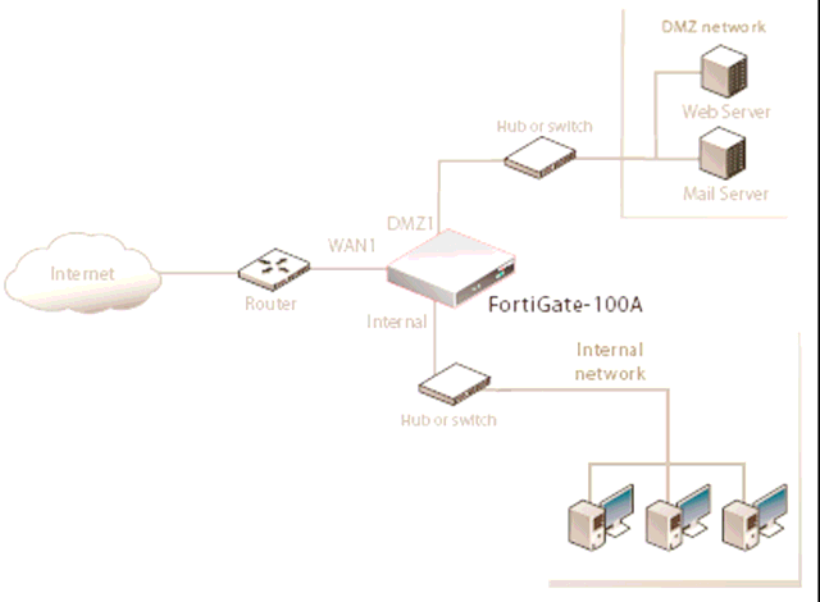
En mode Transparent, le FortiGate n'est pas visible sur le réseau. De même que pour un pont, toutes ses interfaces doivent se trouver sur le même sous-réseau. Il suffit de configurer une adresse IP d'administration pour pouvoir procéder à des modifications dans la configuration et la mise à jour des bases de connaissance antivirus et IPS.

Le mode Transparent d'un FortiGate est généralement utilisé sur un réseau privé derrière un pare-feu ou un routeur existant. Le FortiGate exécute les fonctions de pare-feu, VPN IPSec, analyse de virus, protection d'intrusion et filtrage web et antispam.
Vous pouvez connecter jusqu'à quatre segments réseau au FortiGate afin de contrôler le trafic échangé:

- Un commutateur 4 ports pour connecter l'interface interne du FortiGate au segment réseau interne.
- WAN1 peut se connecter au pare-feu ou routeur externe.
- WAN2, DMZ (DMZ1) et DMZ2 peuvent se connecter à d'autres segments réseau.
- WLAN peut se connecter au LAN sans fil.

Remarque : En mode Transparent, l'interface modem n'est pas disponible sur le FortiGate-60M.

Illustration 9 : Exemple de configuration réseau d'un FortiGate-100A en mode Transparent



Empêcher l'interface publique du FortiGate de répondre aux requêtes ping

La configuration par défaut du FortiGate autorise l'interface publique par défaut de répondre aux requêtes ping. Cette interface, également appelée interface externe publique, est l'interface du FortiGate généralement connectée à Internet.

Pour sécuriser certaines opérations, il est préférable de modifier la configuration de l'interface externe afin que celle-ci ne réponde plus aux requêtes ping. Cette manœuvre empêche la détection du FortiGate à partir d'Internet ce qui sécurise un peu plus le système contre les attaques.

Selon le modèle du boîtier FortiGate, l'interface publique par défaut est soit l'interface externe, soit l'interface WAN1.

Un boîtier FortiGate répond aux requêtes ping lorsque les droits administratifs sont activés en ce sens pour cette interface. Les procédures suivantes permettent d'empêcher un ping d'accéder aux interfaces, externe ou autre, du FortiGate. Ceci fonctionne aussi bien en mode routé qu'en mode Transparent.

Désactiver les droits administratifs ping à partir de l'interface d'administration web

1. Connectez-vous à l'interface d'administration web.
2. Sélectionnez **Système > Réseau > Interface**.
3. Choisissez l'interface externe et cliquez sur Editer.
4. Désactivez la case PING dans les droits d'Administration.
5. Cliquez sur OK pour enregistrer les modifications.

Désactiver les droits administratifs ping à partir de l'interface de ligne de commande

1 Connectez-vous en CLI.

2 Entrez :

```
config system interface
   edit external
     unset allowaccess
  end
```

Installation en mode NAT/Route

Cette section décrit l'installation du FortiGate en mode NAT/Route.

Cette section couvre les sujets suivants:

- Préparation de la configuration du FortiGate en mode NAT/Route
- Configuration DHCP ou PPPoE
- A partir de l'interface d'administration web
- A partir de l'interface de ligne de commande
- Connexion du FortiGate au(x) réseau(x)
- Configuration des réseaux

Préparation de la configuration du FortiGate en mode NAT/Route

Vous pouvez consigner les informations nécessaires à la personnalisation des paramètres du mode NAT/Route dans le tableau 9 de la page 34.

Vous pouvez configurer le FortiGate de deux manières :

- A partir de l'interface d'administration web GUI qui est une interface complète pour configurer la plupart des paramètres. Voir « A partir de l'interface d'administration web » à la page 35.
- A partir de l'interface de ligne de commande (CLI) qui est une interface textuelle complète pour configurer tous les paramètres. Voir « A partir de l'interface de ligne de commande» à la page 36.

Le choix de la méthode dépend de la complexité de la configuration et des types d'accès, d'équipement et d'interface qui vous sont les plus familiers.

Tableau 9 : Paramètres du mode NAT/Route

Mot de passe administrateur:		
Interne	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
WAN1	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
WAN2	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
DMZ	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
DMZ1 (FortiGate-100A)	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
DMZ2 (FortiGate-100A)	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
ADSL (FortiGate-60ADSL)	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
WLAN	IP : Masque de réseau :	_____._____._____._____ _____._____._____._____
Paramètres du réseau	Passerelle par défaut : (Interface connectée au réseau externe)	_____._____._____._____
	Une route par défaut est constituée d'une passerelle par défaut et de l'interface connectée au réseau externe (Internet généralement). Ces paramètres dirigent tout le trafic non local vers cette interface et le réseau externe.	
	Serveur DNS primaire : Serveur DNS secondaire :	_____._____._____._____ _____._____._____._____

Configuration DHCP ou PPPoE

Les interfaces du FortiGate peuvent acquérir leur adresse IP depuis un serveur DHCP ou PPPoE. Votre fournisseur d'accès Internet peut vous fournir des adresses IP via l'un de ces protocoles.

Pour utiliser le serveur FortiGate DHCP, il vous faut configurer pour ce serveur une plage intervalle d'adresses IP et une route par défaut. Ce protocole ne nécessite pas d'autres informations de configuration.

Le protocole PPPoE nécessite, quant à lui, un nom d'utilisateur et un mot de passe. De plus, les configurations non numérotées PPPoE requièrent une adresse IP. Servez-vous du tableau 10 ci-dessous pour consigner les informations nécessaires à la configuration PPPoE.

Tableau 10 : Paramètres PPPoE

Nom d'utilisateur :	
Mot de passe :	

A partir de l'interface d'administration web

Vous pouvez utiliser l'interface graphique pour la configuration initiale du FortiGate et de tous ses paramètres.

Pour plus d'informations sur l'accès à l'interface d'administration web, voir « Accès à l'interface d'administration web » à la page 18.

Configuration des paramètres de base

Après vous être connecté à l'interface d'administration web, vous pouvez utiliser les procédures suivantes pour compléter la configuration de base de votre FortiGate.

Ajouter/modifier le mot de passe administrateur

1. Sélectionnez **Système > Admin > Administrateurs.**
2. Cliquez sur l'icône Changer le mot de passe pour l'administrateur admin.
3. Entrez un nouveau mot de passe et entrez-le une seconde fois pour confirmation.
4. Cliquez sur OK.

Configurer les interfaces

1. Sélectionnez **Système > Réseau > Interface.**
2. Cliquez sur l'icône Editer d'une des interfaces.
3. Choisissez un mode d'adressage : manuel, DHCP ou PPPoE.
4. Complétez la configuration d'adressage.
   - Pour un adressage manuel, entrez l'adresse IP et le masque de réseau de l'interface.
   - Pour un adressage DHCP, sélectionnez DHCP et tous les paramètres requis.
   - Pour un adressage PPPoE, sélectionnez PPPoE et entrez compte utilisateur, mot de passe et autres paramètres requis.

   Pour plus d'informations sur la configuration des paramètres des interfaces, consultez l'aide en ligne FortiGate ou le *Guide d'Administration FortiGate.*
5. Cliquez sur OK.
6. Répétez cette procédure pour chaque interface.

Remarque : Si vous modifiez l'adresse IP de l'interface à laquelle vous êtes connecté, vous devez vous reconnecter à partir d'un navigateur web avec la nouvelle adresse. Connectez-vous à https:// suivi de la nouvelle adresse IP de l'interface. Si la nouvelle adresse IP de l'interface est sur un sous-réseau différent, vous devrez probablement modifier l'adresse IP de votre ordinateur et la configurer sur le même sous-réseau.

Configurer les paramètres du serveur DNS

1. Sélectionnez **Système > Réseau > Options.**
2. Entrez l'adresse IP du serveur DNS primaire.
3. Entrez l'adresse IP du serveur DNS secondaire.
4. Cliquez sur Appliquer.

Ajout d’une route par défaut

Ajouter une route par défaut permet de configurer la destination vers laquelle le FortiGate enverra le trafic destiné au réseau externe (Internet généralement). Cela sert également à définir l’interface connectée au réseau externe. La route par défaut n’est pas requise si cette interface est connectée en DHCP ou PPPoE.

Ajouter une route par défaut

1. Sélectionnez **Routeur > Static > Route statique.**
2. Si le tableau de Route statique stipule une route par défaut (IP et masque configurés à 0.0.0.0), cliquez sur l’icône Supprimer pour effacer cette route.
3. Sélectionnez Créer nouveau.
4. Affectez l’adresse IP destination 0.0.0.0.
5. Affectez le Masque 0.0.0.0.
6. Configurez l’adresse IP de la passerelle par défaut dans le champ Passerelle.
7. Affectez à Interface l’interface connectée au réseau externe.
8. Cliquez sur OK.

Vérification de la configuration à partir de l’interface d’administration web

Pour vérifier les paramètres d’accès, cliquez sur l’interface que vous voulez vérifier et sélectionnez l’icône Editer. Les paramètres sélectionnés lors de la procédure précédente doivent apparaître cochés dans le champ des droits d’administration.

Tester la connexion

La procédure suivante permet de tester la connexion:

- Consultez le site www.fortinet.com
- Importez ou envoyez un courrier électronique de votre boîte aux lettres.

Si vous ne parvenez pas à vous connecter au site web, à importer ou envoyer un courrier électronique, vérifiez la procédure précédente point par point pour vous assurer que toutes les informations ont été entrées correctement. Puis recommencez le test.

A partir de l’interface de ligne de commande

Vous pouvez également configurer votre FortiGate en utilisant les commandes CLI. Pour toute information sur la connexion en CLI, voir « Connexion à partir de l’interface de ligne de commande » à la page 21.

Configuration du FortiGate pour opérer en mode NAT/Route

Reportez-vous aux informations consignées dans le tableau 9 de la page 34 pour accomplir la procédure suivante.

Ajouter/modifier le mot de passe administrateur

1. Connectez-vous en CLI.
2. Pour modifier le mot de passe admin administrateur. Tapez :

```
config system admin
   edit admin
      set password <psswrd>
  end
```

Configurer les interfaces

1 Connectez-vous en CLI.

2 Affectez à l'interface interne l'adresse IP et le masque de réseau tels que consignés au tableau 9 de la page 34. Tapez :

```
config system interface
   edit internal
      set mode static
      set ip <address_ip> <netmask>
  end
```

Exemple

```
config system interface
   edit internal
      set mode static
      set ip 192.168.120.99 255.255.255.0
  end
```

3 Affectez à l'interface externe (WAN1) l'adresse IP et le masque de réseau tels que consignés au tableau 9 de la page 34. Tapez :

```
config system interface
   edit WAN1
      set mode static
      set ip <address_ip> <netmask>
  end
```

Exemple

```
config system interface
   edit WAN1
      set mode static
      set ip 204.23.1.5 255.255.255.0
  end
```

Configurer dynamiquement l'interface WAN1 par DHCP

```
config system interface
   edit WAN1
      set mode dhcp
  end
```

Configurer dynamiquement l'interface WAN1 par PPPoE

```
config system interface
   edit WAN1
      set mode pppoe
      set connection enable
      set username <name_str>
      set password <psswrd>
  end
```

4 Utilisez la même syntaxe pour affecter une adresse IP à chaque interface.

5 Confirmez que les adresses sont correctes. Entrez :

```
get system interface
```

L’interface CLI énumère les adresses IP, masques de réseau et autres paramètres pour chaque port du FortiGate.

Configurer les paramètres du serveur DNS

Configurer les serveurs DNS primaire et secondaire :

```
config system dns
      set primary <address_ip>
      set secondary <address_ip>
  end
```

Exemple

```
config system dns
      set primary 293.44.75.21
      set secondary 293.44.75.22
  end
```

Ajout d’une route par défaut

Ajouter une route par défaut permet de configurer la destination vers laquelle le FortiGate enverra le trafic destiné au réseau externe (Internet généralement). Cela sert également à définir l’interface connectée au réseau externe. La route par défaut n’est pas requise si cette interface est connectée en DHCP ou PPPoE.

Ajouter une route par défaut

Définissez l’adresse IP de la Passerelle par défaut :

```
config router static
     edit 1
       set dst 0.0.0.0 0.0.0.0
       set gateway <gateway_IP>
       set device <interface>
  end
```

Exemple

Si l’IP de la passerelle par défaut est 204.23.1.2 et que celle-ci est connectée à WAN1 :

```
config router static
     edit 1
       set dst 0.0.0.0 0.0.0.0
       set gateway 204.23.1.2
       set device wan1
  end
```

Tester la connexion

La procédure suivante permet de tester la connexion:

- Lancez un ping à destination du boîtier FortiGate.
- Connectez-vous à l’interface graphique GUI.
- Importez ou envoyez un courrier électronique de votre boîte aux lettres.

Si vous ne parvenez pas à vous connecter au site web ou à importer ou envoyer un courrier électronique, vérifiez la procédure précédente point par point pour vous assurer que toutes les informations entrées sont correctes. Puis recommencez le test.

Vous avez maintenant terminé la configuration initiale du FortiGate.

Connexion du FortiGate au(x) réseau(x)

Une fois la configuration initiale terminée, vous pouvez connecter le FortiGate entre le réseau interne et Internet.

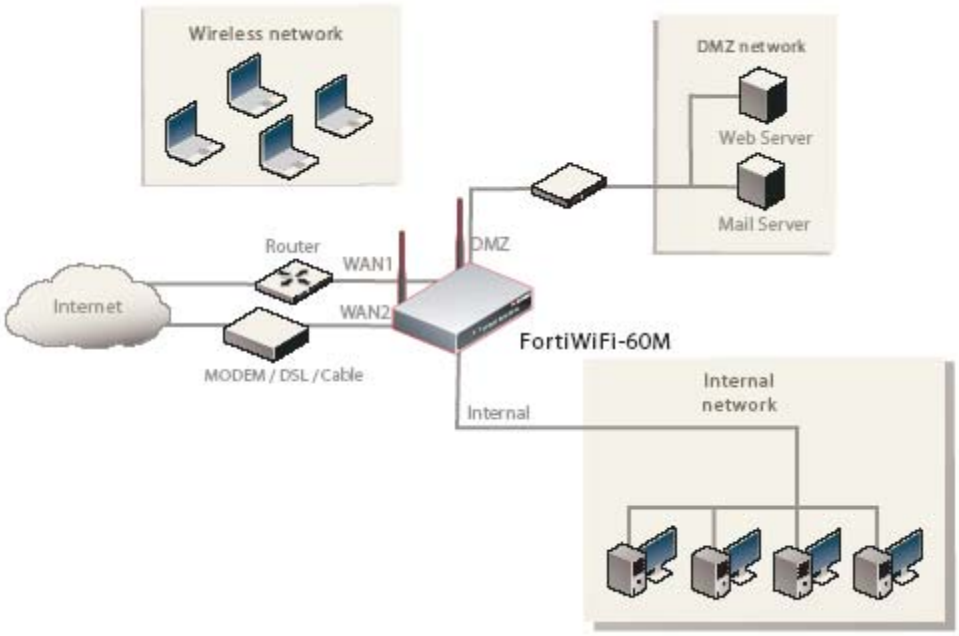
Les connexions réseau disponibles sur le FortiGate sont les suivantes :

- Interne pour la connexion du réseau interne
- WAN1 pour la connexion Internet
- WLAN est l'interface du LAN sans fil sur les modèles FortiWiFi
- DMZ est celle de la DMZ

Se connecter au boîtier FortiGate :

1. Connectez l'interface Interne au concentrateur ou au commutateur du réseau interne.
2. Connectez l'interface Externe à Internet.
   Connectez-vous au commutateur public ou au routeur fourni par votre fournisseur d'accès Internet. Si vous avez une connexion DSL ou câble, connectez l'interface WAN1 à la connexion interne ou LAN de votre modem DSL ou de votre modem câble.
3. Éventuellement vous pouvez aussi connecter l'interface DMZ à votre DMZ.
   Vous pouvez utiliser ce dernier pour fournir un accès à partir d'Internet vers un serveur web ou d'autres serveurs sans que ceux-ci soient connectés au réseau interne.

Illustration 10 : Connexions du FortiWiFi-60M en mode NAT/Route



Configuration des réseaux

En mode routé, vos réseaux doivent être configurés de manière à diriger tout le trafic Internet vers l'adresse IP de l'interface où les réseaux sont connectés.

- Pour le réseau interne, remplacez l'adresse de la passerelle par défaut de tous les ordinateurs et routeurs connectés directement à votre réseau interne par l'adresse IP de l'interface interne du FortiGate.
- Pour la DMZ, remplacez l'adresse de la passerelle par défaut de tous les ordinateurs et routeurs connectés directement à la DMZ par l'adresse IP de l'interface DMZ du FortiGate.
- Pour le réseau WAN, remplacez l'adresse de la passerelle par défaut de tous les ordinateurs et routeurs connectés au réseau WAN1 par l'adresse IP de l'interface WAN du FortiGate.
- Pour le réseau WLAN des boîtiers FortiWiFi-60/60M, configurez une adresse IP pour l'interface réseau de l'aire locale sans fil.

Si vous utilisez le FortiGate comme serveur DHCP pour votre réseau interne, configurez les ordinateurs de votre réseau interne conformément au protocole DHCP.

Assurez-vous que votre boîtier FortiGate fonctionne correctement en vous connectant à Internet à partir d'un ordinateur de votre réseau interne. Vous devriez pouvoir accéder à n'importe quelle adresse Internet.

Installation en mode Transparent

Cette section décrit l'installation du FortiGate en mode Transparent.

Cette section couvre les sujets suivants:

- Préparation de la configuration du FortiGate en mode Transparent
- A partir de l'interface d'administration web
- A partir de l'interface de ligne de commande
- Connexion du FortiGate à votre réseau

Remarque : L'interface ADSL du boîtier FortiGate-60 ADSL ne fonctionne qu'en mode routé et est désactivée en mode Transparent.

Préparation de la configuration du FortiGate en mode Transparent

Reportez-vous au tableau 11 ci-dessous pour consigner les informations nécessaires à la personnalisation des paramètres du mode Transparent.

Deux méthodes permettent la configuration du mode Transparent :

- L'interface d'administration web GUI
- L'interface de ligne de commande (CLI)

Le choix de la méthode dépend de la complexité de la configuration et du type d'accès, d'équipement et d'interface qui vous sont les plus familiers.

Tableau 11 : Paramètres du mode Transparent

Mot de passe Administrateur :		
IP d'administration	IP : Masque de réseau : Passerelle par défaut :	_____._____._____._____ _____._____._____._____ _____._____._____._____
	L'adresse IP et le masque de réseau configurés pour l'administration du boîtier doivent être accessibles depuis le réseau à partir duquel vous allez gérer le FortiGate. Ajoutez une passerelle par défaut si le poste d'administration et le FortiGate ne sont par sur le même sous-réseau.	
Paramétrage DNS	Serveur DNS primaire : Serveur DNS secondaire :	_____._____._____._____ _____._____._____._____

A partir de l'interface d'administration web

Vous pouvez utiliser l'interface d'administration web pour compléter la configuration initiale du FortiGate et de tous ses paramètres.

Pour plus d'informations sur l'accès à l'interface d'administration web, voir « Accès à l'interface d'administration web » à la page 18. La première connexion au FortiGate se fait en mode NAT/Route.

Passer en mode Transparent à partir de l'interface d'administration web

1. Sélectionnez **Système > Statut**.
2. Cliquez sur Modifier à côté du champ Mode de fonctionnement.
3. Sélectionnez Transparent dans la liste Mode de fonctionnement.

Entrez l'adresse IP/Masque de réseau de gestion et l'adresse de la Passerelle par défaut consignées dans le tableau 11 à la page 41.

4 Cliquez sur Appliquer.

Il n'est pas nécessaire de se reconnecter à l'interface d'administration web, les changements sont immédiatement pris en compte en cliquant sur Appliquer. Vous pouvez vérifier le passage en mode Transparent sur le tableau de bord du FortiGate.

Configurer les paramètres du serveur DNS

1 Sélectionnez **Système > Réseau > DNS**.
2 Entrez l'adresse IP du serveur DNS primaire.
3 Entrez l'adresse IP du serveur DNS secondaire.
4 Cliquez sur Appliquer.

A partir de l'interface de ligne de commande

Comme alternative à l'interface graphique, vous pouvez commencer la configuration initiale du FortiGate via les commandes CLI. Pour se connecter en CLI, voir « Connexion à partir de l'interface de ligne de commande » à la page 21. Reportez-vous aux informations consignées dans le tableau 11 de la page 41 pour accomplir les procédures suivantes.

Passer en mode Transparent à partir de l'interface de ligne de commande

1 Assurez-vous d'être connecté en CLI
2 Pour passer en mode Transparent, entrez :

```
config system settings
      set opmode transparent
      set manageip <address_ip> <netmask>
      set gateway <address_gateway>
   end
```

Après quelques secondes, le message suivant s'affiche :

```
Changing to TP mode
```

3 Lorsque le message d'ouverture de la session s'affiche, entrez :

```
get system settings
```

Le CLI affiche le statut du FortiGate notamment l'adresse IP et le masque de réseau de gestion :

```
opmode        : transparent
manageip      : <address_ip><netmask>
```

Assurez-vous de l'exactitude des paramètres du serveur DNS. Ceux-ci étant importés du mode NAT/Route, ils risquent d'être erronés pour la configuration en mode Transparent. Reportez-vous au tableau 11 de la page 41 pour paramétrer le serveur DNS.

Vérifier le paramétrage du serveur DNS

Entrez la commande suivante pour vérifier le paramétrage du serveur DNS FortiGate :

```
show system dns
```

Cette commande CLI donne les informations suivantes:

```
config system dns
     set primary 293.44.75.21
     set secondary 293.44.75.22
```

```
      set fwdintf internal
    end
```

Configurer les paramètres du serveur DNS

Affectez les adresses IP des serveurs DNS primaire et secondaire. Entrez :

```
  config system dns
      set primary <address_ip>
      set secondary <address_ip>
    end
```

Exemple

```
  config system dns
      set primary 293.44.75.21
      set secondary 293.44.75.22
    end
```

Connexion du FortiGate à votre réseau

Une fois la configuration initiale terminée, vous pouvez connecter le FortiGate entre le réseau interne et Internet et connecter un réseau supplémentaire à l'interface DMZ.

La connexion modem des boîtiers FortiGate-60M et FortiGate-60ADSL n'est pas disponible en mode Transparent.

Connecter le boîtier FortiGate en mode Transparent

1. Connectez l'interface Interne au concentrateur ou au commutateur de votre réseau interne.
2. Connectez l'interface WAN1 à un segment du réseau relié au pare-feu ou routeur externe.

   Connectez-vous au commutateur ou au routeur public fourni par votre fournisseur d'accès Internet.
3. Connectez l'interface DMZ à un autre réseau.

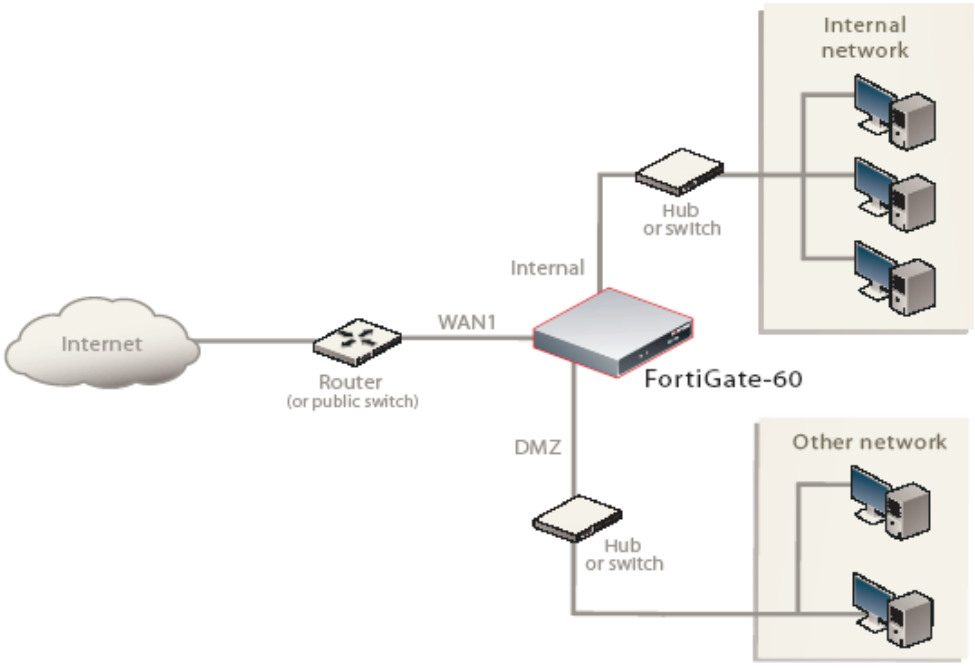
Tester la connexion

La procédure suivante permet de tester la connexion:

- Lancez un ping à destination du boîtier FortiGate.
- Connectez-vous à l'interface d'administration web GUI.
- Consultez ou envoyez un courrier électronique de votre boîte aux lettres.

Si vous ne parvenez pas à vous connecter au site web ou à consulter/envoyer un courrier électronique, vérifiez la procédure précédente point par point pour vous assurer que toutes les informations entrées sont correctes. Puis, recommencez le test.

Illustration 11 : Connexions du FortiGate-60 en mode Transparent



Étapes suivantes

Les instructions suivantes vous permettront de paramétrer la date et l'heure, d'enregistrer le FortiGate et de configurer la mise à jour des bases de connaissance antivirus et IPS.

Reportez-vous au *Guide d'Administration FortiGate* pour obtenir des informations détaillées sur la configuration, le contrôle et la maintenance du FortiGate.

Paramétrage des date et heure

Il est important que la date et l'heure du système du FortiGate soient exactes. Le paramétrage peut se faire soit manuellement, soit automatiquement en configurant le FortiGate pour qu'il se synchronise avec un serveur NTP (Network Time Protocol).

Paramétrer la date et l'heure

1. Sélectionnez **Système > Statut**.
2. Dans **Statut > Heure système**, cliquez sur Changer.
3. Sélectionnez Actualiser pour afficher les date et heure actuelles du système.
4. Sélectionnez votre fuseau horaire dans la liste.
5. Cochez éventuellement « Ajuster automatiquement lors du passage à l'heure d'été / l'heure d'hiver ».
6. Sélectionnez Réglage et réglez la date et l'heure exactes.
7. Réglez heure, minute, seconde, année, mois et jour.
8. Cliquez sur OK.

Remarque : Si vous avez sélectionné l'option « Ajuster automatiquement lors du passage à l'heure d'été / l'heure d'hiver » l'ajustement des date et heure lors du retour à l'heure d'hiver doit se faire manuellement.

Synchronisation des date et heure avec un serveur NTP

1. Sélectionnez **Système > Statut.**
2. Dans **Statut > Heure système**, sélectionnez Changer.
3. Sélectionnez Synchroniser avec le serveur NTP pour un paramétrage automatique des date et heure.
4. Entrez l'adresse IP ou le nom de domaine d'un serveur NTP que le système utilisera pour régler la date et l'heure.
5. Spécifiez l'intervalle de synchronisation.
6. Cliquez sur OK.

Enregistrement de votre FortiGate

Après avoir installé un nouvel équipement FortiGate, enregistrez celui-ci sur le site http://support.fortinet.com en cliquant sur « Product Registration ».

Afin de procéder à l'enregistrement, entrez vos coordonnées et le(s) numéro(s) de série de(s) nouveau(x) boîtier(s) acquis. Plusieurs enregistrements peuvent être introduits lors d'une seule session.

L'enregistrement des nouveaux équipements vous permet d'accéder aux supports techniques et aux mises à jour des bases de données de détection et prévention contre des menaces (Antivirus, Détection d'Intrusion, etc.).

Mise à jour des signatures antivirus et IPS

Vous pouvez configurer le FortiGate pour qu'il se connecte au FortiGuard Distribution Network (FDN – Réseau de Distribution FortiGuard), et mette à jour les bases de connaissance des antivirus, antispam et attaques IPS.

Le FDN est un réseau mondial de FortiGuard Distribution Servers (FDS – Serveurs de Distribution FortiGuard). En se connectant au FDN, le FortiGate se relie au FDS le plus proche grâce à sa liste d'adresses préprogrammées triées en fonction du fuseau horaire sélectionné.

La mise à jour des signatures antivirus et IPS peut se faire soit via l'interface graphique, soit via l'interface de ligne de commande. Pour accéder aux mises à jour votre équipement FortiGate doit avant tout être enregistré. Pour plus d'informations sur l'enregistrement de votre FortiGate, voir « Enregistrement de votre FortiGate » à la page 45.

Remarque : Il est fortement conseillé de mettre les signatures antivirus et IPS régulièrement à jour afin d'éviter que votre FortiGate ne devienne vulnérable face aux nouveaux virus.

Après avoir procédé à l'enregistrement, vérifiez la connexion entre le FortiGate et le FDN :

- Les date et heure doivent être exactes.
- À partir de l'interface d'administration web, sélectionnez « Réactualiser » dans le Centre FortiGuard (FortiGuard Center).

Si la connexion au FDN échoue, recommencez la procédure d'enregistrement de votre FortiGate ou reportez-vous à « Ajout d'un serveur override » à la page 48.

Mise à jour des signatures antivirus et IPS à partir de l'interface d'administration web

Une fois votre équipement FortiGate enregistré, vous pouvez mettre les signatures antivirus et IPS à jour à partir de l'interface d'administration web. Le Centre FortiGuard permet de recevoir des mises à jour par courrier électronique. Pour ce faire, entrez une adresse IP pour la réception de ces courriers et programmez une fréquence de mise à jour hebdomadaire, quotidienne, voire à chaque heure.

Mettre les signatures antivirus et IPS à jour

1 Sélectionnez **Système > Maintenance > FortiGuard Center**.
2 Sélectionnez Mettre à jour.

En cas de succès de connexion au FDN, l'interface d'administration web affiche le message suivant :

```
"Your update request has been sent. Your database will be
updated in a few minutes. Please check your update page for
the status of the update."
```

A savoir:

```
Votre demande de mise à jour a été envoyée. Votre base de
données va être mise à jour dans quelques minutes. Merci de
vérifier le statut de la mise à jour sur la page mise à jour.
```

Lorsqu'une mise à jour est disponible, la page du Centre FortiGuard listera, après quelques minutes, les nouvelles versions d'antivirus, en fonction de leurs dates de

création et numéros de version. Le journal Evénement enregistre les messages témoignant du succès ou de l'échec des mises à jour.

Remarque : La mise à jour des définitions d'antivirus, par l'ajout de nouvelles signatures par FortiGate dans la base de données, peut entraîner une brève rupture du trafic analysé. Il est dès lors préférable de programmer les mises à jour lorsque le trafic est faible, par exemple pendant la nuit.

Mise à jour des signatures IPS à partir de l'interface de ligne de commande

Il est possible de mettre les signatures IPS à jour en utilisant des commandes CLI ci-dessous.

Remarque : La mise à jour des signatures antivirus ne peut se faire qu'à partir de l'interface d'administration web.

Mettre les signatures IPS à jour à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante :

```
configure system autoupdate ips
   set accept-recommended-settings enable
   end
```

Programmation des mises à jour antivirus et IPS

Il est possible de planifier une programmation régulière et automatique des mises à jour des signatures antivirus et IPS, soit via l'interface d'administration web, soit via l'interface de ligne de commande.

Activer la programmation de mises à jour à partir de l'interface d'administration web

1. Sélectionnez **Système > Maintenance > Mise à jour FortiProtect.**
2. Cochez la case Programmation des mises à jour régulières.
3. Sélectionnez une des fréquences suivantes pour la vérification et le téléchargement des mises à jour :

Chaque	La mise à jour a lieu selon un intervalle de temps prédéfini. Sélectionnez le temps souhaité (nombre d'heures, entre 1 et 23 heures) entre chaque demande de mise à jour.
Journalière	La mise à jour a lieu quotidiennement. Vous pouvez en spécifier l'heure précise dans la journée.
Hebdomadaire	La mise à jour a lieu une fois par semaine. Vous pouvez en spécifier le jour et l'heure.

4. Cliquez sur Appliquer.

La nouvelle programmation de fréquence entre en vigueur immédiatement.

A chaque fois que le FortiGate procède à une mise à jour, l'action est enregistrée dans le journal Evénements.

Activer la programmation de mises à jour à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante :

```
config system autoupdate schedule
      set day
      set frequency
      set status
      set time
   end
```

Exemple :

```
config system autoupdate schedule
      set update every Sunday
      set frequency weekly
      set status enable
      set time 16:45
   end
```

Ajout d'un serveur override

Si vous ne parvenez pas à vous connecter au FDN, ou si votre entreprise vous fournit les mises à jour de leur propre serveur FortiGuard, les procédures suivantes vous permettront d'ajouter une adresse IP d'un serveur override FortiGuard soit via l'interface graphique, soit via l'interface de ligne de commande.

Ajouter un serveur override à partir de l'interface d'administration web

1. Sélectionnez **Système > Maintenance > Mise à jour FortiProtect**.
2. Cochez la case Utiliser l'adresse de remplacement.
3. Entrez le nom de domaine entier ou l'adresse IP d'un serveur FortiGuard.
4. Cliquez sur Appliquer.

Le FortiGate teste la connexion vers le serveur override.
En cas de succès, le paramètre du FDN affiche un statut disponible.
Dans le cas contraire où le FDN affiche un statut de service indisponible, le FortiGate n'arrivant pas à se connecter au serveur override, vérifiez les configurations du FortiGate et du réseau et tentez de déceler les paramètres empêchant la connexion au serveur override FortiGuard.

Ajouter un serveur override à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante :

```
config system autoupdate override
      set address
      set status
   end
```

Configuration de l’interface modem

L’interface modem est disponible sur tous les modèles FortiGate série 60, à l’exception du FortiGate-60ADSL.

Les sections suivantes parcourent la configuration du modem du FortiGate-60M à partir de l’interface d’administration web et la configuration des modems des FortiGate-60 et FortiWiFi-60 à partir de l’interface de ligne de commande.

Les FortiGate série 60 supportent une interface modem redondante ou stand alone en mode NAT/Route.

- En mode redondant, l’interface modem prend automatiquement le relais d’une interface Ethernet sélectionnée lorsque celle-ci est indisponible.
- En mode stand alone, l’interface modem sert de connexion entre le FortiGate et Internet.

Lorsque le FortiGate se connecte à un FAI, le modem peut automatiquement appeler jusqu’à trois comptes téléphoniques, et ce jusqu’au moment où la connexion ait lieu.

Cette section couvre les sujets suivants :

- Sélection d’un mode modem
- Configuration des paramètres du modem
- Connexion et déconnexion du modem en mode Stand alone
- Configuration du modem pour les FortiGate-60 et FortiWiFi-60
- Ajout d’un Serveur Ping
- Ajout de règles pare-feu pour les connexions modem

Sélection d’un mode modem

L’interface modem prévoit deux modes de fonctionnement :

- Le mode redondant
- Le mode stand alone

Configuration en mode redondant

L’interface modem redondante sert d’actif en secours d’une interface Ethernet sélectionnée. Si cette dernière se déconnecte de son réseau, le modem se connecte automatiquement aux comptes téléphoniques préconfigurés. Le boîtier FortiGate chemine alors les paquets IP normalement destinés à l’interface Ethernet vers l’interface modem. Tout au long de cette procédure, le boîtier lance des commandes ping à destination de l’interface Ethernet pour vérifier l’état de sa connexion.

Lorsque le boîtier FortiGate détecte que l’interface Ethernet s’est reconnectée au réseau, il déconnecte l’interface modem et repasse sur l’interface Ethernet.

Afin de permettre au boîtier FortiGate de passer de l’interface Ethernet au modem, il est nécessaire, lors de la configuration du modem, de sélectionner cette interface et de lui configurer un serveur ping. De plus, il est important de configurer des

règles pare-feu pour les connexions entre l'interface modem et les autres interfaces du boîtier FortiGate.

Configurer une connexion modem redondante pour le FortiGate-60M

1. Sélectionnez **Système > Réseau > Modem**.
2. Cochez Activer le modem USB.
3. Cochez le mode Redondant.
4. Sélectionnez dans la liste « Actif en secours de » l'interface Ethernet pour laquelle le modem assure le secours.
5. Configurez les autres paramètres du modem requis. Voir « Configuration des paramètres du modem » à la page 51.
6. Configurez un serveur ping pour l'interface Ethernet sélectionnée au point 4. Voir « Ajout d'un serveur Ping » à la page 56.
7. Configurez les règles pare-feu pour les connexions modem. Voir « Ajout de règles pare-feu pour les connexions modem » à la page 56.

Configurer le FortiGate-60 et le FortiWiFi-60 à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante pour configurer un modem redondant :

```
config system modem
      set status enable
      set status mode redundant
   end
```

Configuration en mode stand alone

En mode stand alone, la connexion entre le modem et le compte téléphonique se fait manuellement. L'interface modem est la connexion initiale vers Internet. Le boîtier FortiGate chemine le trafic via l'interface modem, qui reste alors connectée en permanence au compte téléphonique.

Si la connexion vers le compte téléphonique échoue, le modem du boîtier FortiGate recompose automatiquement le numéro du FAI, et ce, autant de fois que spécifié dans la configuration ou jusqu'à ce que la connexion ait lieu.

En mode stand alone, l'interface modem remplace l'interface externe Ethernet. Il est primordial de configurer des règles pare-feu pour les connexions entre l'interface modem et les autres interfaces du boîtier FortiGate.

Remarque : Ne pas ajouter une route par défaut à l'interface Ethernet que l'interface modem remplace.

Remarque : Ne pas ajouter de règles pare-feu pour les connexions entre l'interface Ethernet pour laquelle le modem assure le secours et d'autres interfaces.

Pour que le FortiGate-60M opère en mode stand alone

1. Sélectionnez **Système > Réseau > Modem**.
2. Configurez les autres paramètres du modem requis. Voir « Configuration des paramètres du modem » à la page 51. Assurez-vous de l'exactitude des comptes téléphoniques.

3 Configurez les règles pare-feu pour les connexions vers l'interface modem. Voir « Ajout de règles pare-feu pour les connexions modem » à la page 56.

4 Sélectionnez Appeler.

Le FortiGate commence à composer chaque numéro de téléphone alternativement jusqu'à ce que le modem se connecte à un FAI.

Opérer en mode stand alone à partir de l'interface de ligne de commande

1 Connectez-vous en CLI.

2 Entrez la commande suivante pour configurer un modem en mode stand alone :

```
config system modem
    set status enable
    set status mode standalone
  end
```

3 Entrez la commande suivante pour configurer le compte téléphonique :

```
config system modem
    set auto-dial
    set idle-timeout <minutes_interger>
    set passwd1 <passwrd_srt>
    set phone1 <phone-number_str>
    set redial <tries_interger>
    set username1 <name_str>
  end
```

Configuration des paramètres du modem

La configuration des paramètres du modem permet au boîtier FortiGate d'utiliser le modem pour se connecter jusqu'à trois comptes téléphoniques de votre FAI. Vous pouvez également choisir d'activer ou de désactiver le support du modem FortiGate, de configurer les numéros composés par le modem et de sélectionner l'interface du FortiGate dont le modem assure le secours.

Illustration 12 : Paramètres du modem (Stand alone et Redondant)

Activer le modem USB	Pour activer le modem FortiGate.
État du modem	Les différents statuts du modem sont : « Inactif », « En cours de connexion », « Connecté », « En cours de déconnexion » ou « Déconnecté » (pour le mode Stand alone uniquement).

Appeler/Raccrocher	(Pour le mode Stand alone uniquement). Sélectionnez Appeler pour vous connecter manuellement à un compte téléphonique. Lorsque le modem est connecté, sélectionnez Raccrocher pour déconnecter le modem manuellement.
Mode	Sélectionnez le mode désiré : Standalone ou Redondant. En mode stand alone, le modem est une interface autonome. En mode Redondant, le modem est un outil de sauvegarde, un actif en secours d'une interface Ethernet sélectionnée.
Connexion automatique	(Pour le mode Stand alone uniquement). Appelle le modem automatiquement si la connexion est perdue ou si le boîtier FortiGate redémarre. Cette option n'est pas compatible avec l'option « Connexion à la demande ».
Actif en secours de	(Pour le mode Redondant uniquement). Sélectionnez l'interface Ethernet que le modem doit secourir.
Connexion à la demande	(Pour le mode Stand alone uniquement). Appelle le modem lorsque les paquets sont dirigés vers l'interface modem. Le modem se déconnecte après une période d'inactivité définie dans Timeout d'inactivité. Cette option n'est pas compatible avec l'option « Connexion automatique».
Timeout d'inactivité	(Pour le mode Stand alone uniquement). Etablissez le laps de temps (1-60 minutes) avant qu'une connexion modem inactive soit déconnectée.
Temps d'attente	(Pour le mode Redondant uniquement). Etablissez le laps de temps (1-60 secondes) avant que le FortiGate repasse de l'interface modem vers l'interface initiale, une fois la connexion de celle-ci restaurée. Sélectionnez un temps plus long dans le cas où le FortiGate passe trop fréquemment d'une interface à l'autre.
Nombre d'essais	Sélectionnez le nombre de fois (1 – 10) que le modem du FortiGate tente de se reconnecter au FAI en cas d'échec de connexion. Sélectionnez None pour ne pas limiter le nombre de tentatives d'appel.
Compte téléphonique	Configurez jusqu'à trois comptes téléphoniques. Le FortiGate tente de se connecter à chaque compte alternativement jusqu'à ce que la connexion soit établie.
Numéro de Téléphone	Entrez le numéro de téléphone requis pour la connexion au compte téléphonique. Ne pas inclure d'espace dans les numéros de téléphone. Assurez-vous cependant d'inclure les caractères standard pour les pauses, préfixes de pays, et autres fonctions requises par votre modem pour vous connecter au compte téléphonique.
Compte utilisateur	Le compte utilisateur (maximum 63 caractères) envoyé au FAI.
Mot de passe	Le mot de passe envoyé au FAI.

Le modem se configure et fonctionne uniquement en mode NAT/Route.

Configurer les paramètres du modem

1. Sélectionnez **Système > Réseau > Modem**.
2. Sélectionnez Activer le modem USB.
3. Modifiez les paramètres de la connexion téléphonique.
4. Entrez les paramètres pour le compte téléphonique 1.
5. Si vous avez plusieurs comptes téléphoniques, entrez numéro de téléphone, compte utilisateur et mot de passe pour les comptes téléphoniques 2 et 3.
6. Sélectionnez Appliquer.

Connexion et déconnexion du modem en mode stand alone

Se connecter à un compte téléphonique

1. Sélectionnez **Système > Réseau > Modem**.
2. Sélectionnez Activer le modem USB.
3. Assurez-vous de l'exactitude des comptes téléphoniques.
4. Sélectionnez Appliquer si vous avez apporté des modifications à la configuration.
5. Sélectionnez Appeler.

Le boîtier FortiGate compose alors le numéro de chaque compte téléphonique alternativement jusqu'à ce que le modem se connecte à un FAI.

Inactif	L'interface modem n'est pas connectée à un FAI.
Actif	L'interface modem tente de se connecter à un FAI ou l'est déjà.

Un indicateur vert désigne le compte téléphonique activé.

L'adresse IP et le masque de réseau sont affectés à l'interface modem. Sélectionnez **Système > Réseau > Interface** pour vérifier l'adresse IP et le masque de réseau.

Déconnecter le modem

La procédure suivante permet de déconnecter le modem d'un compte téléphonique.

1. Sélectionnez **Système > Réseau > Modem.**
2. Sélectionnez Raccrocher si vous voulez vous déconnecter du compte téléphonique.

Configuration du modem des FortiGate-60 et FortiWiFi-60

La configuration des paramètres du modem pour le FortiGate-60 et le FortiWiFi-60 se fait à partir de l'interface de ligne de commande. Le tableau suivant reprend les commandes CLI spécifiques à la configuration du modem des FortiGate-60 et FortiWiFi-60.

Tableau 12 : Commandes CLI pour les FortiGate-60 et FortiWiFi-60

Mots-clés et variables	Description	Par défaut
`altmode {enable | disable}`	Permet des installations via PPP en Chine.	`enable`
`auto-dial {enable | disable}`	Permet d'appeler le modem automatiquement en cas de perte de connexion ou à chaque redémarrage du boîtier FortiGate. `dial-on-demand` doit être désactivé et le `mode` sélectionné sur `standalone`.	disable
`connect-timeout <seconds>`	Arrête la recherche de la connexion après x secondes (30 – 255 secondes).	`90`
`dial-on-demand {enable | disable}`	Permet d'appeler le modem lorsque les paquets sont dirigés vers l'interface modem. Le modem se déconnecte après une période `idle-timer`. `auto-dial` doit être désactivé et le `mode` sélectionné sur `standalone`.	disable

Mots-clés et variables	Description	Par défaut
holddown-timer <seconds>	A appliquer seulement si le modem est configuré comme actif en secours d'une interface. Choisissez le temps d'attente (1-60 secondes) avant que le FortiGate repasse de l'interface modem vers l'interface primaire, après que la connexion de celle-ci ait été restaurée. Le mode doit être sur redondant.	60
idle-timer <minutes>	Choisissez le temps d'attente (1-60 minutes) avant qu'une connexion modem inactive soit déconnectée. Le mode doit être sur standalone.	5
interface <name>	Entrez un nom d'interface qui associe l'interface du modem avec l'interface Ethernet secourue (configuration backup) ou à remplacer (configuration stand alone).	No default
mode <mode>	Entrez le mode requis : • standalone L'interface modem est la connexion entre le FortiGate et Internet. • redondant L'interface modem prend automatiquement le relais d'une interface Ethernet sélectionnée lorsque celle-ci est indisponible.	standalone
passwd1 <password_srt>	Entrez le mot de passe pour accéder au compte téléphonique spécifié.	No default
passwd2 <password_srt>	Entrez le mot de passe pour accéder au compte téléphonique spécifié.	No default
passwd3 <password_srt>	Entrez le mot de passe pour accéder au compte téléphonique spécifié.	No default
peer-modem1 {actiontec | ascendTNT | generic}	Sélectionnez Actiontec ou AscendTNT en fonction du type de modem du phone1. Pour tout autre type, sélectionnez generic. Ce paramètre s'applique aux modèles 50AM, 60M, et WiFi-60M.	generic
peer-modem2 {actiontec | ascendTNT | generic}	Sélectionnez Actiontec ou AscendTNT en fonction du type de modem du phone2. Pour tout autre type, sélectionnez generic. Ce paramètre s'applique aux modèles 50AM, 60M, et WiFi-60M.	generic
peer-modem3 {actiontec | ascendTNT | generic}	Sélectionnez Actiontec ou AscendTNT en fonction du type de modem du phone3. Pour tout autre type, sélectionnez generic. Ce paramètre s'applique aux modèles 50AM, 60M, et WiFi-60M.	generic
phone1 <phone-number>	Entrez le numéro de téléphone requis pour vous connecter au compte téléphonique. Ne pas inclure d'espace dans le numéro de téléphone. Assurez-vous d'inclure les caractères standard pour les pauses, préfixes de pays, et autres fonctions requises par votre modem pour vous connecter au compte téléphonique.	No default
phone2 <phone-number>	Entrez le numéro de téléphone requis pour vous connecter au compte téléphonique. Ne pas inclure d'espace dans le numéro de téléphone. Assurez-vous d'inclure les caractères standard pour les pauses, préfixes de pays, et autres fonctions requises par votre modem pour vous connecter au compte téléphonique.	No default

Mots-clés et variables	Description	Par défaut
phone3 <phone-number>	Entrez le numéro de téléphone requis pour vous connecter au compte téléphonique. Ne pas inclure d'espace dans le numéro de téléphone. Assurez-vous d'inclure les caractères standard pour les pauses, préfixes de pays, et autres fonctions requises par votre modem pour vous connecter au compte téléphonique.	No default
redial <tries_interger>	Sélectionnez le nombre de fois (1 – 10) que le FortiGate compose le numéro du FAI pour restaurer une connexion active sur l'interface du modem. Sélectionnez none pour ne pas limiter le nombre de tentatives.	No default
status {disable | enable}	Active ou désactive le support modem.	disable
username1 <name_str>	Entrez le compte utilisateur requis pour accéder au compte téléphonique spécifié.	No default
username2 <name_str>	Entrez le compte utilisateur requis pour accéder au compte téléphonique spécifié.	No default
username3 <name_str>	Entrez le compte utilisateur requis pour accéder au compte téléphonique spécifié.	No default

Exemple

```
config system modem
    set action dial
    set status enable
    set holddown-time 5
    set interface wan1
    set passwd1 acct1passwd
    set phone1 1234567891
    set redial 10
    set username1 acct1user
  end
```

Ajout d’un serveur Ping

L’ajout d’un serveur ping est nécessaire pour la réplication de routage pour le modem en mode redondant. Un serveur ping confirme la connectivité vers une interface Ethernet.

Ajouter un serveur ping à une interface

1. Sélectionnez **Système > Réseau > Interface**.
2. Choisissez une interface et cliquez sur Editer.
3. Dans le champ Ping Serveur entrez l’adresse IP du routeur du prochain saut sur le réseau connecté à l’interface.
4. Cochez la case Activer.
5. Cliquez sur OK pour sauver les modifications.

Détection de l’échec d’une passerelle

Le boîtier FortiGate utilise la détection de l’échec d’une passerelle pour lancer des commandes ping à destination de l’adresse IP du Serveur Ping dans le but de s’assurer que le FortiGate arrive à se connecter à cette adresse IP.

Modifier l’option de détection d’échec d’une passerelle permet de contrôler la confirmation par le FortiGate de la connectivité à l’aide d’un serveur ping ajouté sur une interface. Pour plus d’informations sur l’ajout d’un serveur ping sur une interface, lire « Ajout d’un serveur Ping » ci-dessus.

Modifier les paramètres de détection de l’échec d’une passerelle

1. Sélectionnez **Système > Réseau > Options**.
2. Dans le champ Intervalle de Détection, tapez le laps de temps désiré (en secondes) entre deux lancements de commande ping par le FortiGate.
3. Dans le champ Nombre d’essais avant basculement, entrez le nombre de pings consécutifs perdus à partir duquel le FortiGate considéra la passerelle comme hors service.
4. Cliquez sur Appliquer.

Ajout de règles pare-feu pour les connexions modem

L’interface modem nécessite des adresses et règles pare-feu. Vous pouvez ajouter une ou plusieurs adresses pare-feu à l’interface modem. Pour plus d’informations sur l’ajout d’adresses, lire le *Guide d’Administration FortiGate*. Lorsque de nouvelles adresses sont ajoutées, l’interface modem apparaît dans la matrice de règles.

Vous pouvez configurer des règles pare-feu pour contrôler le flux de paquets circulant entre l’interface modem et les autres interfaces du FortiGate. Pour plus d’informations à propos de l’ajout des règles pare-feu, lire le *Guide d’Administration FortiGate*.

Configuration de l’interface ADSL

L’interface modem ADSL est uniquement disponible sur le FortiGate-60ADSL.

Cette section décrit la configuration de l’interface ADSL d’un boîtier FortiGate-60ADSL et parcourt les différences entre les procédures de configuration de l’interface ADSL et des autres interfaces FortiGate. Pour plus d’informations, reportez-vous au *Guide d’Administration FortiGate*.

Le boîtier FortiGate-60ADSL, équipé d’une interface « Ligne Numérique à Paire Asymétrique » (ADSL), fournit une vitesse de communication plus élevée que les modems téléphoniques standard.

Remarque : L’interface ADSL ne fonctionne qu’en mode NAT/Route. Le passage en mode Transparent désactive l’interface ADSL.

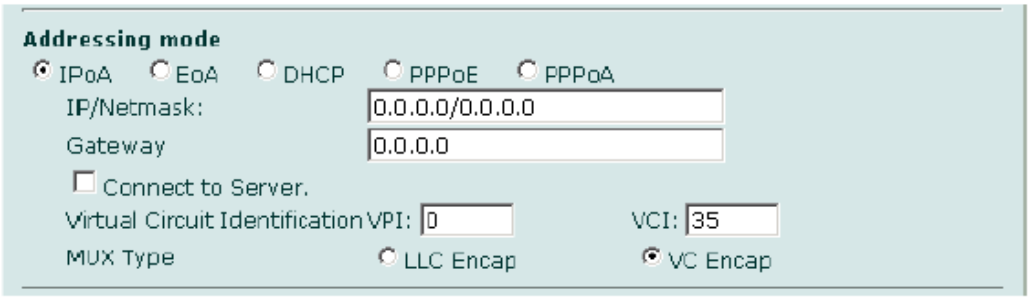
Configuration de l’interface ADSL à partir de l’interface d’administration web

Les procédures suivantes parcourent la configuration de l’interface ADSL et sa connexion à un FAI. Les informations fournies par votre FAI ADSL doivent être entrées aux endroits indiqués.

Configuration des paramètres ADSL de base

L’interface ADSL est configurée de la même manière que toute autre interface réseau physique d’un FortiGate. Les informations à entrer dépendent du mode d’adressage requis par votre FAI. Les adressages statiques utilisant IPOA ou EOA ne nécessitent qu’une adresse IP et un masque de réseau. Pour les adressages dynamiques, reportez-vous aux chapitres « Configuration DHCP de l’interface ADSL » à la page 58 et « Configuration PPPoE ou PPPoA de l’interface ADSL » à la page 59.

Sélectionnez **Système > Réseau > Interface**. Cliquez sur Créer Nouveau ou sélectionnez l’icône Editer d’une interface existante. Dans la section Mode d’adressage, sélectionnez IPoA ou EoA.



Mode d’adressage	Sélectionnez le mode d’adressage requis par votre FAI.
IPoA	IP over ATM. Entrez l’adresse IP et le masque de réseau fournis par votre FAI.

	EoA	Ethernet over ATM, aussi appelé mode Pont. Entrez l'adresse IP et le masque de réseau fournis par votre FAI.
	DHCP	Voir « Configuration DHCP de l'interface ADSL » à la page 58.
	PPPoE	Voir « Configuration PPPoE ou PPPoA de l'interface ADSL » à la page 59.
	PPPoA	Voir « Configuration PPPoE ou PPPoA de l'interface ADSL » à la page 59.
Passerelle		Entrez la passerelle par défaut.
Serveur de connexion		Si activé, l'interface tente automatiquement de se connecter. Désactivez cette option si vous configurez l'interface hors ligne.
Identification du circuit virtuel		Entrez les valeurs VPI et VCI fournies par votre FAI.
Type de MUX		Sélectionnez le type de MUX : LLC Encap ou VC Encap (information fournie par votre FAI).

Pour la configuration requise d'options d'autres interfaces, reportez-vous au *Guide d'Administration FortiGate.*

Configuration DHCP de l'interface ADSL

Si vous choisissez une configuration DHCP pour une interface, le boîtier FortiGate émet automatiquement une requête DHCP. L'interface est configurée avec l'adresse IP et éventuellement les adresses du serveur DNS et l'adresse de la passerelle par défaut fournies par le serveur DHCP.

Sélectionnez **Système > Réseau > Interface** et cliquez ensuite sur Créer Nouveau ou sélectionnez l'icône Editer d'une interface existante. Dans la section Mode d'Adressage, cochez DHCP.

Illustration 13 : Paramètres DHCP de l'interface ADSL

Distance	Entrez la distance administrative de la passerelle par défaut obtenue par le serveur DHCP. La distance administrative, entre 1 et 255, précise la priorité relative d'une route lorsqu'il en existe plusieurs pour une même destination. Au plus bas est la distance administrative, au plus haut est la priorité donnée à la route. La distance par défaut pour la passerelle par défaut est de 1.
Obtenir dynamiquement la route par défaut	Permet d'obtenir l'adresse IP d'une passerelle par défaut à partir d'un serveur DHCP. La passerelle par défaut est ajoutée à la table de routage statique.
Remplacer le serveur DNS préconfiguré	Permet l'utilisation des adresses DNS obtenues par le serveur DHCP à la place des adresses IP du serveur DNS de la page DNS. Vous devrez activer l'option « Obtenir dynamiquement les adresses des serveurs DNS» dans **Système > Réseau > Options**.

Effectuer une requête DHCP	Permet à l'interface de tenter automatiquement de se connecter à un serveur DHCP. Désactiver cette option si vous configurez l'interface hors ligne.

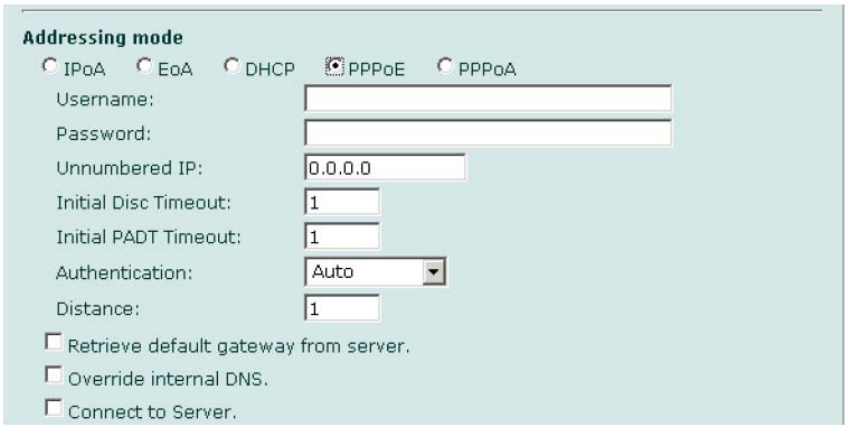
Configuration PPPoE ou PPPoA de l'interface ADSL

Si l'interface est configurée de manière à utiliser PPPoE, le boîtier FortiGate va automatiquement émettre une requête PPPoE. Vous pouvez désactiver « Effectuer une requête PPPoE» si vous configurez le FortiGate hors ligne et ne désirez pas d'envoi de requête PPPoE.

Le boîtier FortiGate supporte de nombreuses fonctions de la RFC PPPoE (RFC 2516) y compris les IP non numérotés, les timeouts de découverte initiale, et les PPPoE Active Discovery Terminate (PADT).

Sélectionnez **Système > Réseau > Interface**. Cliquez sur Créer nouveau ou sur l'icône Editer d'une interface existante. Dans la section Mode d'Adressage, sélectionnez PPPoE ou PPPoA.

Illustration 14 : Paramètres PPPoE ou PPPoA de l'interface ADSL



Entrez les informations suivantes et cliquez ensuite sur Appliquer.

Compte utilisateur	Le nom d'utilisateur du compte PPPoE ou PPPoA fournit par votre FAI.
Mot de passe	Le mot de passe du compte PPPoE ou PPPoA fournit par votre FAI.
Unnumbered IP	Spécifiez l'adresse IP de cette interface. Si votre FAI vous a affecté plusieurs adresses IP, choisissez-en une. Par ailleurs, cette adresse IP peut être identique à celle d'une autre interface ou peut également être n'importe quelle adresse IP.
Initial Disc Timeout	Initial Discovery Timeout. Timeout de découverte initiale. Il s'agit du temps d'attente avant qu'une nouvelle tentative de découverte PPPoE soit lancée. Pour désactiver cette option, assignez-lui 0.
Initial PADT Timeout	Initial PPPoE ou PPPoA Active Discovery Terminate (PADT) timeout. Se définit en secondes. Sert à fermer la session PPPoE ou PPPoA après un laps de secondes d'inactivité défini dans cette option. PADT doit être supporté par votre FAI. Pour désactiver cette option, assignez-lui 0.

Authentification	Sélectionnez la méthode d'authentification utilisée par votre FAI : PAP, CHAP, MSCHAPv1, MSCHAPv2 ou Auto.
Distance	Entrez la distance administrative de la passerelle par défaut obtenue par le serveur PPPoE ou PPPoA. La distance administrative, entre 1 et 255, précise la priorité relative d'une route lorsqu'il en existe plusieurs pour une même destination. Au plus bas est la distance administrative, au plus haut est la priorité donnée à la route. La distance par défaut de la passerelle par défaut est de 1.
Obtenir dynamiquement la route par défaut	Permet d'obtenir l'adresse IP d'une passerelle par défaut à partir d'un serveur PPPoE ou PPPoA. La passerelle par défaut est ajoutée à la table de routage statique.
Remplacer le serveur DNS préconfiguré	Permet de remplacer les adresses IP du serveur DNS de la page DNS par les adresses DNS obtenues par le serveur PPPoE ou PPPoA.
Effectuer une requête	Permet à l'interface de tenter automatiquement de se connecter à un serveur PPPoE ou PPPoA. Désactivez cette option si vous configurez l'interface hors ligne.

Configuration de l'interface ADSL à partir de l'interface de ligne de commande

L'interface ADSL est configurée de la même manière que les autres interfaces physiques FortiGate. Les informations à fournir dépendent du mode d'adressage requis par votre FAI.

Cette section décrit les paramètres disponibles uniquement sur l'interface ADSL et non repris dans les autres documentations FortiGate. De nombreux paramètres s'appliquant aux interfaces s'appliquent généralement aussi à l'interface ADSL. Sont repris ici les seuls paramètres nécessaires pour communiquer avec votre FAI. Pour une liste complète des paramètres interface, référez-vous à `system interface` dans le *Guide de Référence CLI*.

Syntaxe de commande

```
config system interface
   edit adsl
      set ip 10.10.10.1 255.255.255.0
      set mux_type vc-encaps
   ...
   End
```

Mots-clés et variables exclusivement pour l'interface ADSL Ces variables sont uniquement disponibles dans le shell `edit adsl`.		
Mots-clés et variables	**Description**	**Par défaut**
`pppoe-mtu <mtu_bytes>`	Détermine la taille en octets du MTU – quantité de données maximum transmise en une seule unité – pour l'interface ADSL en session PPPoE. Idéalement celui-ci devrait être identique au plus petit MTU de tous les réseaux entre le FortiGate et les destinations des paquets. Intervalle : 576 à 1492	
`gwaddr <gw_ipv4>`	Adresse de la passerelle. Disponible en `mode ipoa ou eoa.`	
`mux_type {llc-encap | vc-encaps}`	Entrez le mode Mux du circuit virtuel.	
`vci`	Entrez l'identificateur du circuit virtuel (VCI) fourni par votre FAI.	35
`vpi`	Entrez l'identificateur du chemin virtuel (VPI) fourni par votre FAI.	0
`auth-type <ppp_auth_method>`	Sélectionnez la méthode d'identification pour PPPoE, PPPoA ou DHCP: • Entrez `auto` pour une sélection automatique de la méthode • Entrez `chap` pour CHAP • Entrez `ms-chapv1` pour Microsoft CHAPv1 • Entrez `ms-chapv2` pour Microsoft CHAPv2 • Entrez `pap` pour PAP `Auth-type` uniquement disponible en `mode pppoe`	`auto`
`connection {enable | disable}`	Active ou désactive la connexion vers un serveur PPPoE ou PPPoA pour la configuration de l'interface. `mode doit être sur dhcp, pppoe ou pppoa`. Disponible en mode NAT/Route uniquement.	`disable`
`defaultgw {enable | disable}`	Active ou désactive l'interface comme passerelle par défaut.	`disable`
`disc-retry-timeout <pppoe_retry_seconds>`	Définit le timeout de découverte initiale en secondes: le temps d'attente avant une nouvelle tentative de découverte PPPoE. Pour désactiver cette option, assignez-lui 0. `mode` doit être sur `pppoe`. Disponible en mode NAT/Route uniquement.	`1`
`dns-server-override {enable | disable}`	Permet à l'interface d'utiliser les adresses du serveur DNS acquises via DHCP ou PPPoE. `mode` doit être sur `dhcp` ou `pppoe`.	`disable`
`edit <interface_name>`	Edite une interface existante ou crée une nouvelle interface VLAN.	Aucun.
`gwdetect {enable | disable}`	Active ou désactive la confirmation de la connectivité avec le serveur à l'adresse IP `detectserver`. La fréquence à laquelle le FortiGate confirme la connectivité est définie par les mots-clés `failtime` et `interval` dans la commande `system global`. Pour plus d'informations, voir le *Guide*	`disable`

Mots-clés et variables exclusivement pour l'interface ADSL Ces variables sont uniquement disponibles dans le shell `edit adsl`.		
Mots-clés et variables	**Description**	**Par défaut**
	de Référence CLI. Disponible en mode NAT/Route uniquement.	
`idle-timeout <pppoe_timeout_seconds>`	Se déconnecte si la connexion PPPoE ou PPPoA est inactive pendant le nombre de secondes défini par cette commande. `mode` doit être sur `pppoe` ou `pppoa`.	0
`ip <interface_ipv4mask>`	Entrez l'adresse IP et le masque de réseau de l'interface. Ceci n'est pas disponible si `mode` est mis sur `dhcp`, `pppoe` ou `pppoa`. Disponible en mode NAT/Route uniquement. L'adresse IP ne peut pas être sur le même sous réseau qu'une autre interface.	
`ipunnumbered <unnumbered_ipv4>`	Activer le mode IP non numéroté pour PPPoE ou PPPoA. Spécifiez l'adresse IP empruntée par l'interface. Cette adresse peut être la même que celle d'une autre interface ou peut être n'importe quelle adresse. Cette option peut être utilisée pour les interfaces PPPoE ou PPPoA pour lesquelles aucune adresse locale unique n'a été fournie. Dans le cas où une plage d'adresses IP vous a été assignée, vous pouvez ajouter n'importe laquelle de ces adresses IP à votre Unnumbered IP.	

`mode <interface_mode>`	Sert à configurer un mode de connexion pour l'interface. Ceci est uniquement disponible en mode NAT/Route.
	`dhcp`
	• Pour recevoir des adresses IP d'un serveur DHCP.
	`pppoe`
	• Pour recevoir des adresses IP d'un serveur PPPoE.
	`pppoa`
	• Pour recevoir des adresses IP d'un serveur PPPoA.
	`eoa`
	• Configure une adresse IP statique pour l'interface en mode ADSL EoA bridge.
	`ipoa`
	• Configure une adresse IP statique pour l'interface en mode ADSL IPoA route.
		`eoa`

`mtu <mtu_bytes>`	Détermine la taille en octets du maximum transmission unit (MTU) – quantité de données maximum transmise en une seule unité. Idéalement celui-ci devrait être identique au plus petit MTU de tous les réseaux entre le FortiGate et les destinations des paquets. En mode `static`, l'intervalle `<mtu bytes>` est de 576 à 1500	1500

Mots-clés et variables exclusivement pour l'interface ADSL Ces variables sont uniquement disponibles dans le shell `edit adsl`.		
Mots-clés et variables	**Description**	**Par défaut**
	octets. En mode `dhcp`, l'intervalle `<mtu_bytes>` est de 576 à 1500 octets. En mode `pppoe`, l'intervalle `<mtu_bytes>` est de 576 à 1492 octets. En mode Transparent, une modification apportée au MTU d'une interface doit être reproduite sur le MTU de toutes les interfaces afin que ces derniers correspondent au nouveau MTU. Cette option est disponible lorsque `mtu-override` est activé.	
`mtu-override {enable | disable}`	Sélectionnez Activer pour utiliser les tailles personnalisées au lieu des tailles par défaut (1500).	`disable`
`padt-retry-timeout <padt_retry_seconds>`	Initial PPPoE ou PPPoA Active Discovery Terminate (PADT) timeout. Se définit en secondes. Sert à éteindre la session PPPoE après un laps de secondes d'inactivité défini dans cette option. PADT doit être supporté par votre FAI. Pour désactiver cette option, assignez-lui 0. `mode` doit être sur `pppoe`. Disponible uniquement en mode NAT/Route.	1
`password <pppoe_password>`	Entrez le mot de passe pour se connecter au serveur PPPoE ou PPPoA. `mode` doit être sur `pppoe` ou `pppoa`. Disponible uniquement en mode NAT/Route.	
`status {down | up}`	Active ou désactive l'interface. En cas de désactivation, l'interface refuse la réception ou l'envoi de paquets. De plus, les interfaces VLAN associées se désactivent également.	up (down pour les VLAN)
`username <pppoe_username>`	Entrez le nom d'utilisateur pour une connexion au serveur PPPoE ou PPPoA. Cette option est disponible en mode NAT/Route lorsque le `mode` est mis sur `pppoe` ou `pppoa`.	

Exemple – IPOA ou EOA

Cet exemple reprend les paramètres requis pour l'utilisation d'une adresse IP de 10.10.10.1 et un masque de réseau de 255.255.255.0 avec un IPOA utilisant PPPoE et des paramètres VPI et VCI personnalisés. Cet exemple peut également s'appliquer au mode EOA si vous changez le paramètre `mode` sur `eoa`.

```
config system interface
   edit adsl
      set mode ipoa
      set ip 10.10.10.1 255.255.255.0
      set vpi 1
```

```
        set vci 34
        set mux-type llc-encaps
        set connection enable
    end
end
```

Exemple – DHCP

Cet exemple reprend les paramètres requis pour se connecter à un FAI via DHCP avec des paramètres par défaut VCI et VPI.

```
config system interface
   edit adsl
      set mode dhcp
      set mux-type llc-encaps
      set connection enable
   end
end
```

Exemple – PPPoE ou PPPoA

Cet exemple reprend les paramètres requis pour se connecter à un FAI utilisant les paramètres par défaut VCI et VPI. Cet exemple peut également s'appliquer au mode PPPoA si vous changez le paramètre `mode` sur `pppoa`.

```
config system interface
   edit adsl
      set mode pppoe
      set username user1
      set password hard_to_guess
      set auth-type pap
      set mux-type llc-encaps
      set connection enable
   end
end
```

Ajout de règles pare-feu pour les connexions ADSL

L'interface ADSL requiert des adresses et des règles pare-feu. Une ou plusieurs adresses peuvent être ajoutées à l'interface ADSL. Pour plus d'informations à ce propos, voir le *Guide d'Administration FortiGate*. Lorsque des adresses sont ajoutées, l'interface ADSL apparaît dans la matrice de règles.

La configuration de règles pare-feu permet de contrôler le flux de paquets entre l'interface ADSL et les autres interfaces d'un boîtier FortiGate. Pour plus d'informations à propos de l'ajout de règles pare-feu, voir le *Guide d'Administration FortiGate.*

Utilisation d’un réseau sans fil

Les informations contenues dans ce chapitre s’appliquent uniquement au FortiWiFi-60.

Dans un réseau câblé, les ordinateurs sont connectés par un ensemble de câbles transmettant les informations. Dans un réseau sans fil, les informations sont transférées par des ondes radio. Certains facteurs peuvent altérer la transmission de données « dans l’air ». Il faut donc les prendre en considération lors de la mise en place d’un réseau sans fil.

Cette section parcourt ces considérations et vous guide dans la mise en place d’un réseau sans fil le plus efficace possible.

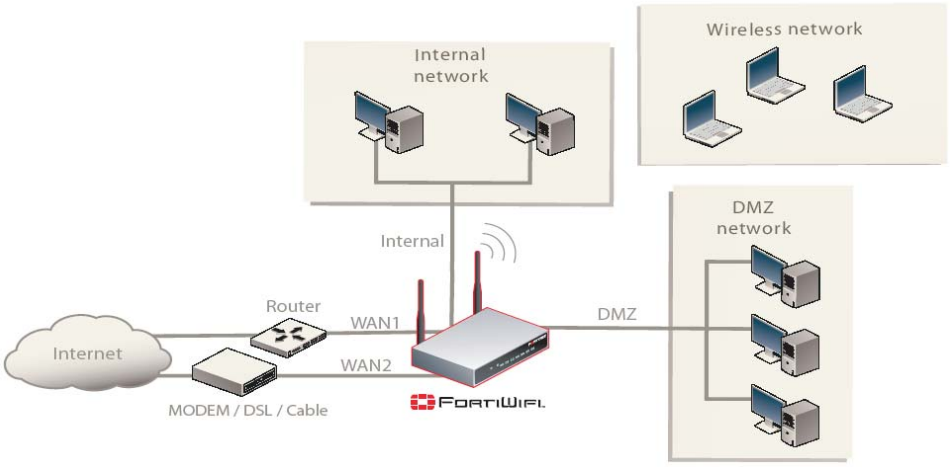
Cette section couvre les sujets suivants:

- Installation d’un réseau sans fil
- Sécurité d’un réseau sans fil
- Modes d’opération sans fil du FortiWiFi-60
- Installation d’un Point d’Accès FortiWiFi-60

Installation d’un réseau sans fil

Dans sa forme la plus simple, un réseau sans fil est un point d’accès communiquant avec un équipement sans fil. Un Point d’Accès (Access Point – AP) est un appareil qui fournit un concentrateur de communication pour un réseau sans fil. L’AP et les appareils sans fil opèrent sur un canal radio commun. Le FortiWiFi-60 agit comme un AP et groupe tous les utilisateurs du réseau sans fil sur le même sous-réseau. Les utilisateurs du réseau sans fil peuvent communiquer sur les réseaux interne et externe (tel qu’Internet) grâce à des règles pare-feu et un routage adaptés.

Illustration 15 : Point d’Accès FortiWiFi-60



Positionnement d’un Point d’Accès

Lors de l’installation d’un FortiWiFi-60 AP, il est essentiel de prévoir que le signal fournit à l’ensemble des utilisateurs soit assez puissant, de manière à assurer une connexion rapide et un transfert de données efficace. Un signal trop faible entraîne un risque d’erreurs dans la transmission de données et la nécessité de renvoyer l’information, ce qui ralentit le transfert.

Les directives suivantes sont à prendre en compte lors de la mise en place d’un FortiWifi-60 AP :

- Des obstacles physiques peuvent entraver le passage de signaux radio. Des objets solides, comme murs et meubles, ou encore des personnes absorbent les ondes radio, ce qui affaiblit le signal. Il vous faut donc tenir compte de ces barrières physiques dans vos espaces bureaux car si les interférences sont trop grandes, le signal n’atteindra pas certaines zones.
- Assurez-vous que le FortiWiFi-60 AP est placé dans un lieu dégagé, dans une pièce où le champ d’activité est maximum, plutôt que dans un coin.
- Les matériaux de construction d’un building peuvent également affaiblir les signaux radio. Les murs en métal affectent la puissance du signal.

Interface Fréquence Radio

Le standard 802.11 utilise un intervalle de fréquences compris entre 2.4 et 2.483 GHz. Une interférence de fréquence radio (radio frequency – RF) se produit lorsque d’autres appareils envoient des signaux radio sur la même fréquence que le FortiWiFi-60 AP. Des appareils sans fil tels que des téléphones sans fil 2.4 GHz, des micro-ondes et des appliances Bluetooth peuvent interférer dans la transmission de paquets sur un réseau sans fil.

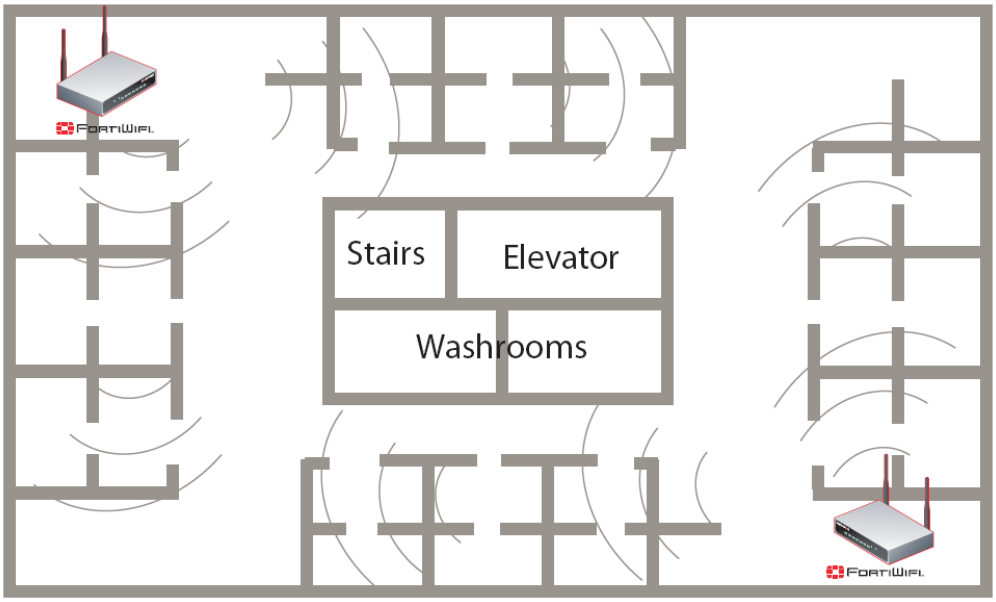
Pour éviter les interférences RF :

- Retirer ces appareils de l’espace de travail. Une simple souris Bluetooth peut causer des interruptions de transmission.
- Maintenez une distance d’au moins 3 mètres (10 pieds) entre les FortiWiFi-60 AP et autres appareils sans fil et les appliances telles que micro-ondes et téléphones sans fil.
- Dans le cas où vous devez travailler avec un téléphone sans fil, choisissez-en un qui n’utilise pas l’intervalle de fréquences 2.4GHz.
- Envisagez plusieurs FortiWiFi-60 AP pour renforcer le signal. Au plus faible est le signal, au plus lente la transmission qui rencontre d’autres appareils sans fil.
- Définir un canal que seuls les utilisateurs et les FortiWiFi-60 AP utilisent peut améliorer la qualité du signal.

Utilisation de multiples Points d’Accès

Si vous ne pouvez éviter certaines de ces contraintes, dues par exemple à l’agencement de vos bureaux ou aux matériaux de construction du bâtiment, vous aurez probablement besoin de plusieurs FortiWiFi-60 AP pour vous aider dans la distribution du signal radio. L’illustration 16 donne un exemple de positionnement de deux FortiWiFi-60 AP destinés à distribuer le signal le plus efficacement possible dans un environnement bureaux tel que représenté ci-dessous :

Illustration 16 : Utilisation de multiples AP pour fournir un signal puissant constant



Dans cet exemple, les bureaux ont des pièces et cages d’escalier et d’ascenseur au centre du bâtiment qui rendent impossible l’utilisation efficace d’un seul FortiWiFi-60 AP. Les métaux de la cage d’ascenseur peuvent causer une dégradation du signal. Dès lors, le placement d’un deuxième FortiWiFi-60 AP dans le coin opposé de la pièce offre une couverture maximum.

Lors de l’utilisation de plusieurs AP, chaque FortiWiFi-60 AP devrait être positionné sur un canal différent pour éviter les interférences dans les endroits où les signaux des deux FortiWiFi-60 AP sont reçus.

Sécurité d’un réseau sans fil

Les ondes radio transmises entre une appliance sans fil et des points d’accès sont des liens souvent peu sécurisés. En effet, la mise en réseau sans fil peut être risquée car l’information est transmise par les ondes radio qui sont un medium public. Le standard 802.11 comprend des options de sécurité qui empêchent vos informations d’être interceptées par des personnes non désirées. Ces moyens sont les systèmes de cryptage Wireless Equivalent Privacy (WEP) et WiFi Protected Access (WPA). Le cryptage sans fil est uniquement utilisé entre l’appliance sans fil et l’AP. L’AP décrypte les données avant de les envoyer sur le réseau câblé. Le FortiWiFi-60 supporte les deux méthodes de cryptage.

Wireless Equivalent Privacy (WEP)

Le système de sécurité WEP utilise un clé de cryptage commune entre l’appliance sans fil et l’AP. Cette clé doit être entrée par l’utilisateur sans fil et l’administrateur.

Une fois activée, l'appliance sans fil crypte les données avec la clé de cryptage pour chaque trame utilisant les codes RSA RC4.

Le système de sécurité WEP est critiqué par certains car ses clés sont statiques et doivent être changées manuellement et régulièrement sur l'appliance sans fil et les AP. Sur un petit réseau, ceci ne pose pas trop de problèmes. Cependant, lorsque le nombre d'utilisateurs et d'AP augmente, le changement régulier des clés WEP peut devenir une tâche administrative lourde entraînant un risque d'erreurs. Dès lors, on observe que les clés sont rarement changées, laissant aux attaquants assez de temps pour s'approprier la clé et accéder au réseau.

Dans les petits réseaux sans fil, le système de sécurité minimisera les infiltrations sur votre réseau et est indiscutablement meilleur que pas de protection du tout. Ceci dit, il est primordial de changer les clés WEP régulièrement, tous les mois au moins, voir toutes les semaines.

Wi-Fi Protected Access (WPA)

Le système WPA a été créé pour remplacer le standard WEP et fournir un meilleur niveau de protection des données dans un réseau sans fil. Ce système prévoit deux méthodes d'authentification : l'authentification 802.1X et les clés partagées.

802.1X authentifie les utilisateurs grâce à un serveur d'authentification EAP de la même manière qu'un serveur RADIUS authentifie chaque utilisateur avant leur connexion au réseau. Les clés de cryptage peuvent être modifiées à des intervalles variables pour minimiser les risques que la clé soit décryptée par des personnes malveillantes.

Dans un environnement réseau où un serveur RADIUS n'est pas une option fiable, le WPA fournit également une authentification à l'aide de clés partagées utilisant le protocole TKIP (Temporal Key Integrity Protocol). Ce protocole permet à la clé de cryptage d'être continuellement renégociée pendant la connexion de l'utilisateur au réseau sans fil. De cette manière une clé unique est créée pour chaque paquet. Pour assurer davantage encore l'intégrité de vos données, un MIC (Message Integrity Code) est incorporé dans chaque paquet à l'aide d'un code d'intégrité de message de 8 octets cryptés à partir de l'adresse MAC et des données.

Le système WPA fournit une sécurité plus robuste entre les appliances sans fil et les points d'accès. Les boîtiers FortiWiFi-60/60M supportent ces deux méthodes.

Mesures de sécurité additionnelles

Le FortiWiFi-60 est fourni avec des mesures de sécurité supplémentaires qui permettent de bloquer l'accès à votre réseau sans fil aux utilisateurs non désirés. L'installation de ces options complémentaires assurera d'autant plus de sécurité à votre réseau.

Filtrage des adresses MAC

Pour améliorer la sécurité de votre réseau sans fil, vous pouvez activer le filtrage des adresses MAC sur le FortiWiFi-60. Cette option permet de définir les appliances sans fil qui ont le droit d'accéder au réseau en fonction de leur adresse MAC. Lorsqu'un utilisateur tente de se connecter au réseau sans fil, le boîtier FortiWiFi-60 compare l'adresse MAC de l'utilisateur avec sa propre liste. Si l'adresse MAC se trouve sur la liste des adresses autorisées, l'utilisateur accède au réseau. Dans le cas contraire, l'utilisateur est rejeté. Le filtrage d'adresses MAC complique la tâche aux attaquants qui tentent de se connecter au réseau sans fil via des adresses MAC aléatoires.

Service Set Identifier

Le Service Set Identifier (SSID) définit le nom du réseau sans fil partagé par les utilisateurs. Ceux-ci doivent configurer leur ordinateur de manière à se connecter au réseau qui émet ce nom. Pour des raisons de sécurité, il est vivement conseiller de modifier le nom par défaut « fortinet » de votre réseau.

La diffusion permet aux utilisateurs du réseau sans fil de trouver un réseau. Les modèles FortiWiFi-60 offrent l'option de ne pas émettre le SSID. Ce qui garantit un peu plus la protection du réseau. Si la configuration de tous les utilisateurs du réseau sans fil se fait sur un SSID correct, il n'est pas nécessaire de diffuser le SSID.

Désactiver le SSID

1. Sélectionnez **Système > Wireless > Paramètres**.
2. Sélectionnez Désactiver pour le SSID Broadcast.
3. Cliquez sur OK.

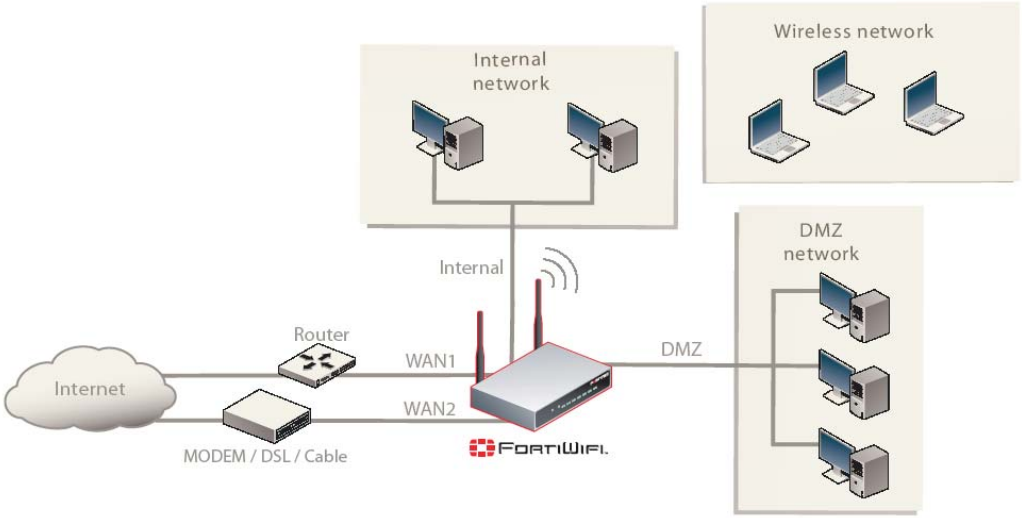
Modes d'opération sans fil du FortiWiFi-60

Les FortiWiFi-60 opèrent avec deux modes d'opération pour les réseaux sans fil : Point d'accès et Client.

Mode Point d'Accès

En mode Point d'Accès, le boîtier sert de point d'accès auquel plusieurs utilisateurs peuvent se connecter, envoyer et recevoir des informations sur un réseau sans fil, sans connexion physique. Le FortiWiFi-60 peut se connecter au réseau interne et agir comme un pare-feu contre Internet. Le mode Point d'accès est le mode par défaut.

Illustration 17 : Un boîtier FortiWiFI-60 en mode Point d'Accès



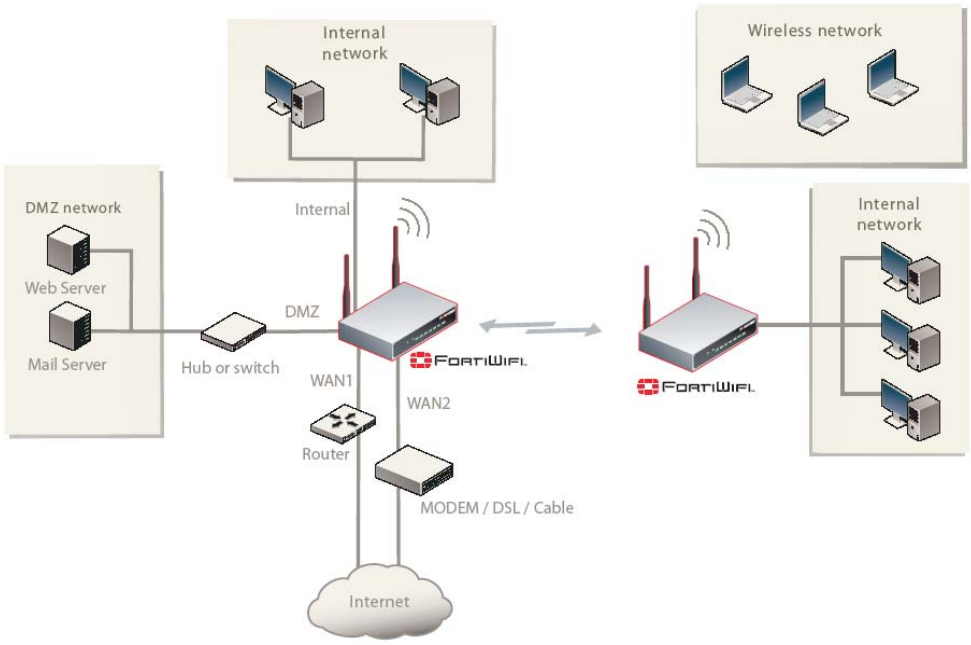
Mode Client

En mode Client, le boîtier est défini pour recevoir des transmissions d'un autre point d'accès. Cela permet aux utilisateurs à distance de se connecter à un réseau existant grâce à l'utilisation de protocoles sans fil, à partir d'un endroit qui ne possède pas d'infrastructure câblée.

Par exemple, l'agencement d'un entrepôt se prête difficilement à un réseau câblé quand les lieux d'envois et de réception sont à des côtés opposés du bâtiment. Le

FortiWiFi-60 peut supporter les utilisateurs câblés grâce à ses quatre ports Ethernet et peut se connecter sans fil à un autre Access Point en tant que client. Cela permet aux utilisateurs du réseau câblé de se connecter en utilisant le standard 802.11 comme point d'appui.

Illustration 18 : Le boîtier FortiWiFi-60/60M en mode Client



Changement de mode d'opération sans fil

Changer le mode d'opération sans fil

1. Sélectionnez **Système > Wireless > Paramètres**.
2. Dans Mode d'Opération, cliquez sur Changer.
3. Sélectionnez le mode d'opération sans fil désiré et cliquez sur OK.

Installation d'un Point d'Accès FortiWiFi-60

Cette section décrit comment configurer rapidement le FortiWiFi-60 pour en faire un Point d'Accès qui permettra aux postes de travail sans fil, localisés sur le même LAN sans fil que le boîtier, d'accéder au réseau. Seront également parcourus dans ce chapitre : la configuration de règles pare-feu et les consignes de sécurité pour assurer un environnement sans fil sécurisé. Pour initier l'installation, connectez un ordinateur configuré en TCP/IP comme client DHCP sur le réseau interne.

Cette section parcourt les sujets suivants :

- Mise en place des paramètres DHCP
- Mise en place des options de sécurité
- Configuration des règles pare-feu

Mise en place des paramètres DHCP

Il est nécessaire de configurer un serveur DHCP pour l'interface WLAN du FortiWiFi-60. Tout comme un serveur DHCP, l'interface affecte dynamiquement des adresses IP aux équipements du réseau connecté à l'interface WLAN.

Configurer le FortiWiFi-60/60M pour en faire un serveur DHCP

1. Sélectionnez **Système > DHCP > Service**.
2. Cliquez sur le triangle bleu pour accéder aux options WLAN.
3. Configurez les paramètres du serveur DHCP :

Nom	Entrez un nom au serveur DHCP. Par exemple, DHCPServer_1.
Activer	Active le serveur DHCP.
Type	Sélectionnez régulier sauf si la configuration concerne des clients à distance qui utiliseront une connexion IPSec VPN vers l'interface WLAN.
Intervalle IP	Entrez l'adresse IP du WLAN pour configurer l'intervalle d'adresses IP. Par exemple, 10.10.80.1 à 10.10.80.20.
Masque de réseau	Entrez le masque de réseau consigné dans le Tableau 9 de la page 34.
Domaine	Entrez le nom de domaine, par exemple, www.fortinet.com.
Date d'expiration	La date d'expiration d'une adresse IP. Cette option permet de préciser une limite dans le temps d'une adresse IP.
Avancées	Uniquement pour spécifier plusieurs serveurs DNS (y compris les serveurs WIN) pour une interface.

4. Cliquez sur OK.

Remarque : L'intervalle IP doit concorder avec l'adresse du sous-réseau où la requête DHCP a été reçue. Généralement il s'agit du sous-réseau connecté à l'interface WLAN.

Mise en place des options de sécurité

Pour garantir une sécurité et une protection adaptées à votre réseau et aux informations, il est nécessaire de mettre en place des options de sécurité sur le FortiWiFi-60.

Mettre en place les options de sécurité

1. Sélectionnez **Système > Wireless > Paramètres**.
2. Entrez un SSID.
3. Activez ou désactivez le SSID Broadcast.
4. Sélectionnez un Mode de Sécurité.
5. Entrez une clé ou une clé partagée en fonction du Mode de Sécurité sélectionné.
6. Sélectionnez la case MAC Filter.
7. Activez le filtrage des MAC si désiré.
8. Entrez les adresses MAC et sélectionnez pour chacune l'action Accepter ou Rejeter.

Remarque : Les informations entrées aux points 2 et 5 doivent être transmises aux utilisateurs du réseau sans fil afin qu'ils puissent s'y connecter.

Remarque : Il est fortement conseillé de ne pas sélectionner « None » car cela rend votre réseau plus vulnérable aux attaques.

Configuration des règles pare-feu

Le FortiWiFi-60 est équipé d'interfaces WAN pour connexions Internet. Les connexions Internet peuvent être configurées d'une part pour les réseaux câblés sur les interfaces interne et/ou DMZ, d'autre part pour le réseau sans fil, sur l'interface WLAN.

La création de règles pare-feu permet un accès Internet sécurisé pour les clients du réseau sans fil à partir de l'interface WLAN vers les interfaces WAN1 ou WAN2.

Dans l'exemple suivant, une règle pare-feu pour les clients du réseau sans fil (interface WLAN) qui se connectent à Internet (interface WAN1) est créée, utilisant le traffic shaping, l'authentification pare-feu et les règles par défaut de vérification stricte de contenu.

Créer une nouvelle règle pare-feu pour une connexion Internet sécurisée

1. Sélectionnez **Pare-feu > Règle**.
2. Cliquez sur la flèche bleue WLAN -> WAN1.
3. Cliquez sur Créer Nouveau.

   Configurez les paramètres suivants :

Source Interface/Zone	WLAN
Source Address	All
Destination Interface/Zone	WAN1
Destination Address	All
Horaire	always
Service	ANY
Action	ACCEPT
NAT	Activé
Profil de protection	Strict

4. Sélectionnez Avancé.
5. Sélectionnez Traffic Shaping.
6. Configurez les paramètres de la bande passante du Traffic Shaping et le Niveau de priorité selon vos besoins.
7. Sélectionnez OK.

Logiciel FortiGate

Fortinet met régulièrement le logiciel FortiGate à jour en y intégrant des améliorations et résolutions aux problèmes d'adresses. Une fois votre FortiGate enregistré, le logiciel peut être téléchargé sur le site http://support.fortinet.com.

Seuls les administrateurs FortiGate (dont le profil prévoit tous les droits d'accès en lecture et écriture du système) et les utilisateurs admin FortiGate peuvent modifier le logiciel FortiGate.

Cette section parcourt les sujets suivants:

- Mise à jour logicielle
- Retour à une version logicielle antérieure
- Mise à jour logicielle à partir d'un redémarrage système et par ligne de commande
- La clé FortiUSB
- Test d'une nouvelle version logicielle avant son installation
- Installation et utilisation d'une image logicielle de sauvegarde (FortiGate-100A uniquement)

Remarque : Si vous avez une version antérieure du logiciel FortiOS, par exemple FortiOS v2.50, procédez à la mise à jour vers FortiOS v2.80MR11 avant la mise à jour vers FortiOS v3.0.

Mise à jour logicielle

Vous pouvez utiliser, au choix, l'interface d'administration web ou l'interface de ligne de commande pour la mise à jour logicielle FortiOS.

Mise à jour logicielle à partir de l'interface d'administration web

Les procédures suivantes permettent d'installer une nouvelle version logicielle sur le FortiGate.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

Mettre le logiciel à jour à partir de l'interface d'administration web

1. Copiez le fichier de l'image logicielle sur votre poste d'administration.
2. Connectez-vous à l'interface d'administration web en tant qu'administrateur admin.
3. Sélectionnez **Système > Statut**.
4. Dans **Statut > Version de code**, sélectionnez Update (Mettre à jour).

5. Tapez le chemin et le nom de fichier de l'image logicielle, ou sélectionnez « Browse » (Parcourir) pour localiser ce fichier.
6. Cliquez sur OK.

   Le FortiGate télécharge le fichier de l'image logicielle, installe la nouvelle version logicielle, redémarre et affiche la page d'ouverture d'une session FortiGate. Cette procédure prend quelques minutes.
7. Connectez-vous à l'interface d'administration web.
8. Sélectionnez **Système > Statut** et vérifiez la version du code pour vous assurer du succès de l'installation de la mise à jour.
9. Mettez les bases de connaissance antivirus et IPS à jour. Pour plus d'informations sur ce sujet, reportez-vous au *Guide d'Administration FortiGate*.

Mise à jour logicielle à partir de l'interface de ligne de commande

La procédure suivante nécessite un serveur TFTP connecté au FortiGate.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Vous pouvez également utiliser la commande CLI `execute update-now` pour mettre à jour ces définitions. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

Mettre le logiciel à jour à partir de l'interface de ligne de commande

1. Assurez-vous que le serveur TFTP est opérationnel.
2. Copiez le fichier de la nouvelle image logicielle sur le répertoire racine du serveur TFTP.
3. Connectez-vous en CLI.
4. Veillez à ce que le FortiGate se connecte bien au serveur TFTP.

   Vous pouvez utiliser la commande suivante pour lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

   ```
   execute ping 192.168.1.168
   ```
5. Entrez la commande suivante pour copier l'image logicielle du serveur TFTP vers le FortiGate :

   ```
   execute restore image TFTP <name_str> <tftp_ipv4>
   ```

   où `<name_str>` est le nom du fichier de l'image logicielle, et `<tftp_ip4>` est l'adresse IP du serveur TFTP. Par exemple, si le nom du fichier de l'image logicielle est `image.out` et l'adresse IP du serveur TFTP est 192.168.1.168, entrez :

   ```
   execute restore image image.out 192.168.1.168
   ```

   Le FortiGate répond par le message suivant:

   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```

   A savoir :

   ```
   Cette opération va remplacer la version logicielle actuelle !
   ```

```
Voulez-vous continuer ? (oui/non)
```

6. Tapez y.

   Le FortiGate télécharge le fichier de l'image logicielle, met à jour la version logicielle et redémarre. Cette procédure prend quelques minutes.
7. Reconnectez-vous en CLI.
8. Pour vous assurer du succès de l'installation de l'image logicielle, entrez :
   ```
   get system status
   ```
9. Mettez les bases de connaissance antivirus et IPS à jour. Pour ce faire, entrez :
   ```
   execute update-now
   ```
   Egalement lire à ce propos le *Guide d'Administration FortiGate*.

Retour à une version logicielle antérieure

Les procédures suivantes permettent d'équiper le FortiGate d'une version antérieure du logiciel.

Vous pouvez utiliser, au choix, l'interface d'administration web ou l'interface de ligne de commande pour retourner à une version précédente du logiciel. Cette procédure restaure la configuration par défaut du FortiGate.

Retour à une version logicielle antérieure à partir de l'interface d'administration web

Les procédures suivantes entraînent la restauration de la configuration par défaut sur le FortiGate et la suppression des signatures personnalisées IPS, de la base de données de filtrage web et antispam et des changements apportés aux messages de remplacement.

Avant de commencer ces procédures, il est recommandé de :

- sauvegarder la configuration du FortiGate
- sauvegarder les signatures personnalisées IPS
- sauvegarder la base de données de filtrage web et antispam

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

Retourner à une version logicielle antérieure à partir de l'interface d'administration web

1. Copiez le fichier de l'image logicielle sur votre poste d'administration.
2. Connectez-vous à l'interface d'administration web du FortiGate.
3. Sélectionnez **Système > Statut**.

4 Dans **Statut > Version du code**, sélectionnez « Update » (Mettre à jour).
5 Tapez le chemin et le nom du fichier de l'image logicielle, ou sélectionnez « Browse » (Parcourir) pour localiser ce fichier.
6 Cliquez sur OK.
Le FortiGate télécharge le fichier de l'image logicielle, retourne à la version antérieure du logiciel, redémarre et affiche la page d'ouverture d'une session FortiGate. Cette procédure prend quelques minutes.
7 Connectez-vous à l'interface d'administration web.
8 Sélectionnez **Système > Statut** et vérifiez la version du code pour vous assurer du succès de l'installation du logiciel.
9 Restaurez votre configuration.
Pour plus d'informations sur la restauration de votre configuration, reportez-vous au *Guide d'Administration FortiGate*.
10 Mettez à jour les bases de connaissance antivirus et IPS.
Pour plus d'informations sur les définitions des antivirus et attaques, reportez-vous au *Guide d'Administration FortiGate*.

Retour à une version logicielle antérieure à partir de l'interface de ligne de commande

Cette procédure entraîne la restauration de la configuration par défaut sur le FortiGate et la suppression des signatures personnalisées IPS, de la base de données de filtrage web et antispam et des changements apportés aux messages de remplacement.

Avant de commencer cette procédure, il est recommandé de :

- sauvegarder la configuration du système FortiGate en entrant la commande `execute backup config`
- sauvegarder les signatures personnalisées IPS en entrant la commande `execute backup ipsuserdefsig`
- sauvegarder la base de données de filtrage web et antispam

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*. Vous pouvez également entrer la commande `execute update-now` pour mettre les bases de connaissance antivirus et IPS à jour.

Remarque : La procédure suivante nécessite que vous vous connectiez à partir du compte administrateur admin ou d'un compte administrateur qui possède tous les droits d'accès en lecture et écriture de la configuration du système.

La procédure suivante nécessite un serveur TFTP connecté au FortiGate.

Retourner à une version logicielle antérieure à partir de l'interface de ligne de commande

1. Assurez-vous que le serveur TFTP est opérationnel.
2. Copiez le fichier de l'image logicielle sur le répertoire racine du serveur TFTP.
3. Connectez-vous en CLI.
4. Veillez à ce que le FortiGate se connecte bien au serveur TFTP.
   Vous pouvez utiliser la commande suivante pour lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :
   `execute ping 192.168.1.168`
5. Entrez la commande suivante pour copier l'image logicielle du serveur TFTP vers le FortiGate :
   `execute restore image TFTP <name_str> <tftp_ipv4>`
   où `<name_str>` est le nom du fichier de l'image logicielle, et `<tftp_ip4>` est l'adresse IP du serveur TFTP. Par exemple, si le nom du fichier de l'image logicielle est `v28image.out` et l'adresse IP du serveur TFTP est 192.168.1.168, entrez :
   `execute restore image TFTP v28image.out 192.168.1.168`

   Le FortiGate répond par le message suivant:

   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```

   A savoir :
   ```
   Cette opération va remplacer la version logicielle actuelle !
   Voulez-vous continuer ? (oui/non)
   ```
7. Tapez `y`.
   Le FortiGate télécharge le fichier de l'image logicielle. Après le téléchargement du fichier un message similaire à celui ci-dessous s'affiche :
   ```
   Get image from tftp server OK.
   Check image OK.
   This operation will downgrade the current firmware version!
   Do you want to continue? (y/n)
   ```

   A savoir:
   ```
   Image bien reçue du serveur tftp.
   Contrôle de l'image OK.
   Cette opération va rétrograder votre version logicielle actuelle !
   Voulez-vous continuer ? (oui/non)
   ```
8. Tapez `y`.
   Le FortiGate retourne à l'ancienne version logicielle, restaure la configuration par défaut et redémarre. Cette procédure prend quelques minutes.
9. Reconnectez-vous en CLI.
10. Pour vous assurer du succès du téléchargement de l'image logicielle, entrez :
    `get system status`
11. Pour restaurer votre configuration précédente, si nécessaire, utilisez la commande :
    `execute restore config TFTP <name_str> <tftp_ipv4>`

12 Mettez les bases de connaissance antivirus et IPS à jour à partir de l'interface de ligne de commande, en entrant :

```
execute update-now
```

Egalement, pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Mise à jour logicielle à partir d'un redémarrage système et par ligne de commande

Cette procédure permet d'installer un logiciel spécifié et de restaurer la configuration par défaut du FortiGate. Vous pouvez utiliser cette procédure pour mettre à jour une version logicielle, retourner vers une version antérieure ou encore réinstaller la version actuelle.

Cette procédure nécessite une connexion en CLI à partir du port de la console FortiGate et un câble série RJ-45 <> DB-9. Cette procédure restaure la configuration par défaut du FortiGate.

Remarque : Cette procédure diffère en fonction des versions BIOS FortiGate. Ces différences, lorsqu'elles sont d'application, sont précisées dans les étapes concernées de la procédure ci-dessous. La version du BIOS du FortiGate peut être visualisée par une connexion en port console lors du redémarrage du boîtier.

Cette procédure nécessite :

- Un accès en CLI via une connexion au port de la console FortiGate avec un câble série RJ-45 <> DB-9.
- L'installation d'un serveur TFTP auquel vous pouvez vous connecter à partir de l'interface interne du FortiGate. Ce serveur doit être sur le même sous-réseau que l'interface interne.

Avant de commencer cette procédure, il est recommandé de :

- sauvegarder la configuration du FortiGate
- sauvegarder les signatures personnalisées IPS
- sauvegarder la base de données de filtrage web et antispam

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate.*

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

Remarque : Les bases de connaissance antivirus et IPS sont remplacées par celles de la nouvelle version logicielle. Après la mise à jour logicielle, assurez-vous que ces bases de connaissance sont à jour. Pour plus de détails, reportez-vous au *Guide d'Administration FortiGate*.

Mettre à jour une version logicielle à partir d'un redémarrage système

1 Connectez-vous en CLI en utilisant les ports du câble série RJ-45 <> DB-9 et de la console FortiGate.

2 Assurez-vous que le serveur TFTP est opérationnel.

3 Copiez le fichier de la nouvelle image logicielle sur le répertoire racine du serveur TFTP.

4 Veillez à ce que l'interface interne soit connectée au même réseau que le serveur TFTP.

5 Pour vous assurer de la connexion du FortiGate au serveur TFTP, utilisez la commande suivante pour lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

```
execute ping 192.168.1.168
```

6 Entrez la commande suivante pour redémarrer le FortiGate.

```
execute reboot
```

Le FortiGate répond par le message suivant:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

A savoir :

```
Cette opération va réinitialiser le système !
Voulez-vous continuer ? (oui/non)
```

7 Tapez y.

Pendant le démarrage du FortiGate, une série de messages s'affiche sur l'écran.

Appuyez immédiatement sur une touche du clavier pour interrompre le démarrage du système lorsqu'un des messages suivants apparaît :

- Pour un FortiGate muni d'un BIOS v2.x

```
Press Any Key To Download Boot Image ....
..
```

- Pour un FortiGate muni d'un BIOS v3.x

```
Press any key to display configuration menu ..............
......
```

Remarque : Vous n'avez que 3 secondes pour appuyer sur une touche. Si vous n'appuyez pas à temps, le FortiGate se réinitialise et vous devez ré-entrer dans le système et recommencer la commande `execute reboot`.

Si vous avez interrompu avec succès le processus de démarrage, un des messages suivants apparaît :

- Pour un FortiGate muni d'un BIOS v2.x

```
Enter TFTP Server Address [192.168.1.168]:
```

Passez alors au point 9.

- Pour un FortiGate muni d'un BIOS v3.x

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G, F, Q, or H:
```

8 Tapez G pour accéder à la nouvelle image logicielle à partir du serveur TFTP.

Le message suivant apparaît :

```
Enter TFTP server address [192.168.1.168]:
```

9 Entrez l'adresse du serveur TFTP et appuyez sur la touche Enter :

Le message suivant apparaît :

```
Enter Local Address [192.168.1.188]:
```

10 Entrez une adresse IP que le FortiGate peut utiliser pour se connecter au serveur TFTP. Il peut s'agir de n'importe quelle adresse IP valide pour le réseau auquel est connectée l'interface. Veillez à ne pas entrer une adresse IP d'un autre équipement de ce réseau.

Le message suivant apparaît :

```
Enter File Name [image.out]:
```

11 Entrez le nom de fichier de l'image logicielle et appuyez sur Enter.

Le serveur TFTP télécharge le fichier sur le FortiGate et un message similaire apparaît :

- Pour un FortiGate muni d'un BIOS v2.x

  ```
  Do You Want To Save The Image ? [Y/n]
  ```

  Tapez Y.

- Pour un FortiGate muni d'un BIOS v3.x

  ```
  Save as Default firmware/Run image without saving:[D/R]
  ```

  ou

```
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]
```

12 Tapez D.

Le FortiGate installe la nouvelle image logicielle et redémarre. L'installation peut prendre plusieurs minutes.

Restauration de la configuration précédente

Si nécessaire, modifiez l'adresse de l'interface interne via la commande CLI suivante :

```
config system interface
    edit internal
        set ip <address_ipv4mask>
        set allowaccess {ping https ssh telnet http}
    end
```

Après avoir modifié l'adresse de l'interface, vous pouvez accéder au FortiGate à partir de l'interface graphique et restaurer la configuration :

- Restaurer la configuration du FortiGate
- Restaurer les signatures personnalisées IPS
- Restaurer le filtrage web
- Restaurer la base de données de filtrage antispam
- Mettre à jour les bases de connaissance antivirus et IPS

Pour plus d'informations, reportez-vous au *Guide d'Administration FortiGate*.

Si vous retournez à une version antérieure FortiOS (par exemple, passer de FortiOS v3.0 à FortiOS v2.80), la configuration antérieure risque de ne pas pouvoir être restaurée à partir de la sauvegarde du fichier de configuration.

La clé FortiUSB

La clé FortiUSB garantit flexibilité et contrôle lors de la sauvegarde de fichiers de configuration ou de l'installation de nouvelles images logicielles. La clé FortiUSB permet :

- l'installation d'images logicielles
- la sauvegarde et restauration de fichiers de configuration
- l'auto-installation d'un fichier de configuration ou image à partir d'un redémarrage système.

La clé FortiUSB est compatible avec le port USB de tout ordinateur, vous permettant de télécharger directement des images logicielles sur la clé. En insérant la clé USB dans le port USB du boîtier FortiGate, vous pouvez sauvegarder un fichier de configuration existant et installer une nouvelle image logicielle sur d'autres boîtiers FortiGate.

Remarque : La clé FortiUSB est vendue séparément. Seules les clés FortiUSB provenant de chez Fortinet sont compatibles avec les boîtiers FortiGate.

Mise à jour logicielle à partir de la clé FortiUSB

Vous pouvez utiliser la clé FortiUSB pour mettre à jour facilement et rapidement votre boîtier FortiGate.

Mettre à jour une image logicielle à partir de la clé USB

1. Insérez la clé USB dans le port USB de votre ordinateur.
2. Téléchargez sur votre clé FortiUSB la nouvelle version logicielle qui se trouve sur le site de Fortinet à l'adresse : http://support.fortinet.com .
3. Insérez la clé FortiUSB dans le port USB du boîtier FortiGate.
4. A partir de l'interface d'administration web, sélectionnez **Système > Statut > Information > Version de code.**
5. Cliquez sur Mettre à jour et ensuite sur Browse (Parcourir).
6. Sélectionnez le fichier du logiciel téléchargé sur votre clé FortiUSB et cliquez sur Open (ouvrir).
7. Cliquez sur OK.

Remarque : Veillez à ce que le boîtier FortiGate soit éteint avant de retirer la clé FortiUSB, ceci pour éviter tout risque pour le système.

Vous pouvez maintenant tester la nouvelle version logicielle. Pour ce faire, suivez la procédure décrite dans le chapitre « Test d'une nouvelle version logicielle avant son installation » à la page 84.

Sauvegarde et restauration à partir de la clé FortiUSB

La clé FortiUSB permet de sauvegarder une image logicielle existante ou encore de restaurer la dernière image logicielle présente sur votre boîtier FortiGate. Il est également possible de crypter le fichier de configuration, lors d'une sauvegarde sur votre ordinateur ou sur la clé FortiUSB. Avant de commencer, assurez-vous que votre clé FortiUSB est bien insérée dans le port USB du boîtier FortiGate.

Remarque : Veillez à ce que le boîtier FortiGate soit éteint avant de retirer la clé FortiUSB, ceci afin d'éviter tout risque pour le système.

Remarque : Les certificats VPN peuvent être enregistrés uniquement si vous cryptez le fichier. Assurez-vous que le cryptage de la configuration est sélectionné pour vous permettre d'enregistrer les certificats VPN avec le fichier de configuration.

Sauvegarder la configuration FortiGate à partir de l'interface d'administration web

1. Sélectionnez **Système > Maintenance > Sauvegarde et Restauration**.
2. Sélectionnez un disque USB dans la liste Sauvegarde de la configuration sur
3. Nommez le fichier de configuration.
4. Sélectionnez Sauvegarder (Backup)

Restaurer la configuration FortiGate à partir de l'interface d'administration web

1. Sélectionnez **Système > Maintenance > Sauvegarde et Restauration**.
2. Sélectionnez un disque USB dans la liste Restauration de la configuration à partir de.
3. Sélectionnez un fichier de configuration de sauvegarde de la liste.
4. Sélectionnez Restaurer (Restore).

Sauvegarder la configuration FortiGate à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante pour sauvegarder les fichiers de configuration :

   ```
   exec backup config usb <filename>
   ```
3. Entrez la commande suivante pour vérifier que les fichiers de configuration sont sur la clé:

   ```
   exec usb-disk list
   ```

Restaurer la configuration FortiGate à partir de l'interface de ligne de commande

1. Connectez-vous en CLI.
2. Entrez la commande suivante pour restaurer les fichiers de configuration :

```
exec restore image usb <filename>
```

Le FortiGate répond par le message suivant:

```
This operation will replace the current firmware
version!
Do you want to continue? (y/n)
```

A savoir :

```
Cette opération va remplacer la version logicielle
actuelle !
Voulez-vous continuer ? (o/n)
```

3 Tapez y.

A partir de la fonction d'auto-installation USB

La fonction d'auto-installation USB permet à chaque redémarrage système de mettre à jour les fichiers de configuration et d'images. Il s'agit de plus d'une sauvegarde supplémentaire si jamais vous devriez éteindre ou réinitialiser le FortiGate tout en désirant maintenir les mêmes paramètres du système.

Configurer la fonction d'auto-installation USB à partir de l'interface d'administration web

1 Sélectionnez **Système > Maintenance > Sauvegarde et Restauration**.

2 Cliquez sur la flèche bleue pour afficher les options avancées.

3 Cochez les options suivantes :

- Quand le système redémarre, mettre à jour la configuration de la FortiGate par celle de la clé USB si le Fichier de Configuration par défaut est présent sur celle-ci.
- Quand le système redémarre, mettre à jour le Firmware de la FortiGate par celle de la clé USB si l'Image par défaut est présente sur celle-ci.

4 Entrez les noms de fichiers de configuration et d'image ou utiliser le nom de fichier de configuration par défaut (system.conf) et le nom de l'image par défaut (image.out).

5 Cliquez sur Appliquer.

Configurer la fonction d'auto-installation USB à partir de l'interface de ligne de commande

1 Connectez-vous en CLI.

2 Entrez les commandes suivantes :

```
config system auto-install
        set default-config-file <filename>
        set auto-intall-config <enable/disable>

        set default-image-file <filename>
        set auto-install-image <enable/disable>
```

```
end
```

3 Entrez la commande suivante pour voir les paramètres de l'installation du nouveau logiciel :
```
get system status
```

Commandes CLI supplémentaires pour l'utilisation de la clé FortiUSB

Les commandes CLI suivantes vous permettent de supprimer un fichier de la clé FortiUSB, inventorier les fichiers présents sur la clé, formater la clé ou encore de renommer un fichier :

- `exec usb-disk list`
- `exec usb-disk delete <filename>`
- `exec usb-disk format`
- `exec usb-disk rename <filename1> <filename2>`

Remarque : À partir commandes CLI, pour supprimer de la clé FortiUSB un fichier de configuration dont le nom contient des espaces, insérez des guillemets de part et d'autre du nom du fichier.

Test d'une nouvelle version logicielle avant son installation

Vous pouvez tester une nouvelle version logicielle en l'installant en mémoire lors du redémarrage système. Après avoir accompli cette procédure, le FortiGate opère sous la nouvelle version logicielle avec la configuration actuelle. Cette nouvelle version n'est pas installée définitivement. Au prochain démarrage du FortiGate, celui-ci opèrera sous la version logicielle d'origine avec sa configuration actuelle. Si la nouvelle version logicielle fonctionne bien, vous pouvez l'installer définitivement en suivant la procédure « Mise à jour logicielle » à la page 73.

Il est recommandé d'utiliser cette procédure de test avant d'installer une nouvelle version logicielle. Pour appliquer cette procédure, vous avez besoin de vous connecter en CLI via le port de la console FortiGate et le câble série RJ-45 <> DB-9. Cette procédure installe temporairement une nouvelle version logicielle sous votre configuration actuelle.

Cette procédure nécessite :

- Un accès en CLI en connectant le port de la console FortiGate avec un câble série RJ-45 <> DB-9.
- L'installation d'un serveur TFTP connecté à l'interface interne du FortiGate. Ce serveur doit être sur le même sous-réseau que l'interface interne

Tester une version logicielle

1 Connectez-vous en CLI en utilisant le câble série RJ-45 <> DB-9 et le port de la console FortiGate.

2 Assurez-vous que le serveur TFTP est opérationnel.

3 Copiez le fichier de la nouvelle image logicielle sur le répertoire racine du serveur TFTP.

4 Veillez à ce que l'interface interne soit connectée au même réseau que le serveur TFTP.

Vous pouvez lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

```
execute ping 192.168.1.168
```

5 Entrez la commande suivante pour redémarrer le FortiGate :

```
execute reboot
```

6 Pendant la réinitialisation du FortiGate, appuyez sur une touche du clavier pour interrompre le démarrage du système. Alors que le FortiGate démarre, une série de messages s'affiche sur l'écran.

Lorsqu'un des messages suivants apparaît, appuyez immédiatement sur une touche du clavier pour interrompre le démarrage du système :

- Pour un FortiGate muni d'un BIOS v2.x

```
Press Any Key To Download Boot Image ....
......
```

- Pour un FortiGate muni d'un BIOS v3.x

```
Press any key to display configuration menu ..............
......
```

Remarque : Vous n'avez que 3 secondes pour appuyer sur une touche. Si vous n'appuyez pas à temps, le FortiGate se réinitialise et vous devez ré-entrer dans le système et recommencer la commande `execute reboot`.

7 Si vous avez interrompu avec succès le processus de démarrage, un des messages suivants apparaît :

- Pour un FortiGate muni d'un BIOS v2.x

```
Enter TFTP Server Address [192.168.1.168]:
```

Passez alors au point 9.

- Pour un FortiGate muni d'un BIOS v3.x

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G, F, Q, ou H:
```

8 Tapez `G` pour accéder à la nouvelle image logicielle à partir du serveur TFTP.

Le message suivant apparaît :

```
Enter TFTP server address [192.168.1.168]:
```

9 Entrez l'adresse du serveur TFTP et appuyez sur la touche Enter :

Le message suivant apparaît :

```
Enter Local Address [192.168.1.188]:
```

10 Entrez une adresse IP que le FortiGate peut utiliser pour se connecter au serveur TFTP.

L'adresse IP doit se trouver sur le même réseau que le serveur TFTP. Cependant, veillez à ne pas entrer une adresse IP d'un autre équipement de ce réseau.

Le message suivant apparaît :

```
Enter File Name [image.out]:
```

11 Entrez le nom de fichier de l'image logicielle et appuyez sur la touche Enter.

Le serveur TFTP télécharge le fichier sur le FortiGate et un message similaire apparaît :

- Pour un FortiGate muni d'un BIOS v2.x

```
Do You Want To Save The Image ? [Y/n]
```

Tapez n.

- Pour un FortiGate muni d'un BIOS v3.x

```
Save as Default firmware/Run image without saving:[D/R]
```

ou

```
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]
```

12 Tapez R.

L'image logicielle est installée en mémoire et le FortiGate fonctionne sous la nouvelle version logicielle, mais avec sa configuration actuelle.

13 Vous pouvez vous connecter en CLI ou à l'interface d'administration web en utilisant n'importe quel compte administrateur.

14 Pour vous assurer du succès du téléchargement de la nouvelle image logicielle, entrez à partir des commandes CLI :

```
get system status
```

Vous pouvez maintenant tester la nouvelle image logicielle.

Installation et utilisation d'une image logicielle de sauvegarde

Les procédures parcourues dans ce chapitre s'appliquent uniquement au FortiGate-100A.

Sous la version BIOS v3.x, vous pouvez installer une image logicielle de sauvegarde. Une fois cette image installée, vous pouvez y revenir chaque fois que nécessaire.

Installation d'une image logicielle de sauvegarde

Cette procédure nécessite :

- L'accès à l'interface de ligne de commande en connectant le câble RJ-45 <> DB-9au port de la console FortiGate.
- L'installation d'un serveur TFTP auquel le FortiGate peut se connecter en suivant la procédure décrite dans « Mise à jour logicielle à partir d'un redémarrage système et par ligne de commande » à la page 78.

Installer une image logicielle de sauvegarde

1 Connectez-vous en CLI en utilisant les ports du câble RJ-45 <> DB-9 et de la console FortiGate.

2 Assurez-vous que le serveur TFTP est opérationnel.

3 Copiez le fichier de la nouvelle image logicielle sur le répertoire racine du serveur TFTP.

4 Pour vous assurer de la connexion du FortiGate au serveur TFTP, vous pouvez utiliser la commande suivante pour lancer un ping à destination du serveur TFTP. Par exemple, si l'adresse IP du serveur TFTP est 192.168.1.168 :

```
execute ping 192.168.1.168
```

5 Entrez la commande suivante pour redémarrer le FortiGate.

```
execute reboot
```

Pendant le démarrage du FortiGate, une série de messages s'affiche sur l'écran.

6 Appuyez immédiatement sur une touche du clavier pour interrompre le démarrage du système lorsque le message suivant apparaît :

```
Press any key to enter configuration menu .........
```

Remarque : Vous n'avez que 3 secondes pour appuyer sur une touche. Si vous n'appuyez pas à temps, le FortiGate se réinitialise et vous devez ré-entrer dans le système et recommencer la commande `execute reboot`.

Si vous avez interrompu avec succès le processus de démarrage, le message suivant apparaît :

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G, F, Q, or H:
```

7 Tapez `G` pour accéder à la nouvelle image logicielle à partir du serveur TFTP.

Le message suivant apparaît :

```
Enter TFTP server address [192.168.1.168]:
```

8 Entrez l'adresse du serveur TFTP et appuyez sur la touche Enter :

Le message suivant apparaît :

```
Enter Local Address [192.168.1.188]:
```

9 Entrez une adresse IP que le FortiGate peut utiliser pour se connecter au serveur TFTP.

Il peut s'agir de n'importe quelle adresse IP valide pour le réseau auquel est connectée l'interface. Veillez à ne pas entrer une adresse IP d'un autre équipement de ce réseau.

Le message suivant apparaît :

```
Enter File Name [image.out]:
```

10 Entrez le nom de fichier de l'image logicielle et appuyez sur Enter.

Le serveur TFTP télécharge le fichier sur le FortiGate et le message suivant apparaît :

```
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]
```

11 Tapez `B`.

Le FortiGate enregistre la nouvelle image logicielle et redémarre. Lorsque le FortiGate redémarre, il fonctionne sous la version précédente de l’image logicielle.

Index

—A—

ajout d'un serveur override 48
ajout d'un serveur ping 56
ajout d'une route par défaut 36, 38

—C—

certificat de sécurité 18
clé FortiUSB 81
  fonction d'auto-installation 83
  mise à jour logicielle 81
  sauvegarde et restauration 82
CLI
  connexion 21
configuration
  DHCP 34
  PPPoE 34
configuration par défaut
  des profils de protection 27
  du pare-feu 26
  en mode NAT/Route 25
  en mode Transparent 26
  installation rapide 22
connexion
  à l'interface d'administration web 18
  à partir de l'interface de ligne de commande 21

—D—

date et heure
  paramétrage 45
DHCP
  configuration 34
diodes électroluminescentes 17

—E—

enregistrement du FortiGate 45

—F—

FortiGate
  documentation 11
FortiGate-60ADSL
  configuration 57
Fortinet
  Base de Connaissance 13
  Service clientèle et support technique 13
Fortinet, gamme de produits
  FortiAnalyser 8
  FortiBridge 8
  FortiClient 8

FortiGuard 7
FortiMail 8
FortiManager 9
FortiReporter 8
fuseaux horaires 45

—I—

interface ADSL
configuration à partir de l'interface d'administration web 57
configuration à partir de l'interface de ligne de commande 60
configuration DHCP 58
configuration PPPoE ou PPPoA 59
interface d'administration web
connexion 18
interface de ligne de commande
connexion 21

—L—

logiciel FortiGate 73
mise à jour 73
mise à jour
à partir de l’interface d’administration web 73
mise à jour
à partir de l’interface de ligne de commande 74
retour à une version antérieure 75
retour à une version antérieure
à partir de l’interface d’administration web 75
retour à une version antérieure
à partir de l’interface de ligne de commande 76
test d'une nouvelle version avant son installation 84

—M—

mise à jour
des signatures antivirus et IPS 46
logicielle 73
logicielle
à partir de l’interface d’administration web 73
logicielle
à partir de l’interface de ligne de commande 74
logicielle
à partir d’un redémarrage système et par ligne de commande 78
mise à jour logicielle
à partir de la clé FortiUSB 81
mode NAT/Route 29
à partir de l'interface d'administration web 35
à partir de l'interface de ligne de commande 36
paramètres 33–34
mode Transparent 31
à partir de l'interface d'administration web 41
à partir de l'interface de ligne de commande 42

paramètres 53
modem
commandes CLI 53
configuration 53
connexion et déconnexion 53
mode redondant 49
mode stand alone 50
paramètres 51

—N—

NAT/Route, mode 29
NTP, serveur
synchronisation 45

—P—

paramétrage par défaut
restauration 28
PPPoE
configuration 34
produits de la gamme Fortinet 7
profils de protection 27

—R—

requêtes ping
empêcher de répondre 32
réseau sans fil
installation 65
modes d'opération 69
sécurité 67
restauration
du paramétrage par défaut 28
restauration de la configuration précédente 80
retour à une version logicielle antérieure 75
à partir de la clé FortiUSB 82
à partir de l'interface d'administration web 75
à partir de l'interface de ligne de commande 76

—S—

sauvegarde d'une image logicielle
à partir de la clé FortiUSB 82
service clientèle et support technique 13
synchronisation des date et heure
avec un serveur NTP 45

—T—

tableau de bord 20
Transparent, mode 31